SECURITY ADVISORY

SPR-2609082, Issue 1

8 September 2026

Sprecher Automation GmbH
Franckstrasse 51, 4020 Linz / Austria
T: +43 732 6908-0
F: +43 732 6908-278
info@sprecher-automation.com
www.sprecher-automation.com

Contents

Wibu Systems-103401: Vulnerabilities in CodeMeter Runtime If Configured as Server

1. Summary

Sprecher Automation has been notified by WIBU-Systems of several security vulnerabilities in the WIBU-Systems CodeMeter Runtime.

CodeMeter Runtime is only affected by the vulnerabilities listed below if it is configured as a server. This is not the default.
To verify the setting:

- Open the CodeMeter Control Center, open WebAdmin, go to menue "Configuration/Server/Server Access". Check the Radio Button "Network Server"
  - Enable — configured as a server (affected).
  - Disable — not configured as a server.
- or check the profiling value "IsNetworkServer" in the Registry Editor "Computer\HKEY_LOCAL_MACHINE\SOFTWARE\WIBU-SYSTEMS\CodeMeter\Server\CurrentVersion":
  - IsNetworkServer=1 — configured as a server (affected).
  - IsNetworkServer=0 — not configured as a server.

1.1. Vulnerabilities

Improper Access Control in Local-Only Configuration Commands (CVE-2026-81573)
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.
CWE-284: Improper Access Control

Format String Vulnerability in Logger (CVE-2026-81574)
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.
CWE-134: Use of Externally-Controlled Format String

Missing Sanity Checks for Buffer Lengths (CVE-2026-81575)
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.

CWE-130: Improper Handling of Length Parameter Inconsistency

Improper Authentication of Session Handles (CVE-2026-81576)
If configured as a server, CodeMeter Runtime issues handles per connection and relies on a cryptographically weak 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.
CWE-639: Authorization Bypass Through User-Controlled Key

2. Affected Products and Versions

SPRECON-V460 versions running CodeMeter Runtime versions 6.x or 7.x or 8.x-versions < 8.41a or 9.x-versions < 9.10.

3. Workarounds and Mitigations

Improper Access Control in Local-Only Configuration Commands (CVE-2026-81573)
Upgrade CodeMeter Runtime 8.x versions to >= 8.41a
Upgrade CodeMeter Runtime 9.x versions to >= 9.10

Workaround
If you enabled the network server functionality at some point but no longer need it, disable it:
If you are using CodeMeter 9.00 or newer, you can use cmu --disable-network-server
If you are using older versions of CodeMeter, do the following:

- Open the CodeMeter Control Center, open WebAdmin, go to menue "Configuration/Server/Server Access". Set the Radio Button "Network Server" to "Disable"
- or
    - On Windows, open the Registry Editor and navigate to Computer\HKEY_LOCAL_MACHINE\SOFTWARE\WIBU-SYSTEMS\CodeMeter\Server\CurrentVersion, then change the value of IsNetworkServer from 1 to 0. Restart CodeMeter.
    - On Linux and Mac, first stop CodeMeter, then edit the file under /etc/wibu/CodeMeter/Server.ini. Under [General], change the value IsNetworkServer from 1 to 0. Then start CodeMeter again.

Format String Vulnerability in Logger (CVE-2026-81574)
See Workarounds & Mitigations CVE-2026-81573

Missing Sanity Checks for Buffer Lengths (CVE-2026-81575)
See Workarounds & Mitigations CVE-2026-81573

Improper Authentication of Session Handles (CVE-2026-81576)
See Workarounds & Mitigations CVE-2026-81573

4. Vulnerability Classification

CVE ID: **2026-81573**
CVSS 3.1 Score: 8.6
CVSS Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:H/A:L

CVE ID: **2026-81574**
CVSS 3.1 Score: 8.2
CVSS Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:H

CVE ID: **2026-81575**
CVSS 3.1 Score: 7.5
CVSS Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H

CVE ID: **2026-81576**
CVSS 3.1 Score: 7.7
CVSS Vector: CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:C/C:H/I:N/A:N

The CVE® programme identifies, defines and catalogues publicly disclosed cyber security vulnerabilities. Vulnerabilities are discovered, assigned and published by organisations from around the world that have partnered with the CVE® programme. (Copyright © The MITRE Corporation https://www.cve.org/Legal/TermsOfUse)

CVSS is an open assessment framework that can be used to indicate the characteristics and severity of software vulnerabilities, whereby this is not a measure of risk. This standard is documented on the website https://www.first.org/cvss/.

5. General Security Recommendations

Sprecher Automation recommends compliance with common safety recommendations of general and industry-specific standards and norms. E. g.:

- to restrict local physical access to authorised persons only
- keeping the operating system and software up to date
- using application whitelisting to restrict the execution of applications to those required for the operation of the system
- testing updated versions in a test environment to verify normal operation of the system according to the project-specific configuration and hardware environment before installing the update in a production environment
- that a disaster recovery plan is in place to reverse the installation of the update if unexpected problems occur in the production environment after the update has been installed

6. Sprecher Automation PSIRT

Sprecher Automation has a **Product Security and Incident Response Team (PSIRT)** to reduce risks, increase cyber security in products and resolve IT security incidents. If you or your company have found a cybersecurity vulnerability in Sprecher Automation products, please contact us at the functional address security@sprecher-automation.com. (If you need an S/MIME certificate for encrypted communication, you can send an email with the subject "Certificate Request" to this address).

7. Document History

2026-09-08 Publication date