SECURITY ADVISORY

SPR-2609081, 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

CVE-2026-81572: Wibu Systems-103081: Local Privilege Escalation in CodeMeter Runtime on Windows

1. Summary

Sprecher Automation has been notified by WIBU-Systems of a vulnerability in the WIBU-Systems CodeMeter Runtime.

This affects the CodeMeter Universal Support Tool (cmu.exe), which is used to manage and maintain CodeMeter licenses and CmContainers.
"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

CWE-59: Improper Link Resolution Before File Access
https://cwe.mitre.org/data/definitions/59.html

2. Affected Products and Versions

SPRECON-V460 versions running CodeMeter Runtime versions 8.x-versions 8.40 - 8.41 or 9.x-versions < 9.10.

3. Workarounds and Mitigations

Upgrade CodeMeter Runtime 8.x versions to >= 8.41a
Upgrade CodeMeter Runtime 9.x versions to >= 9.10

4. Vulnerability Classification

CVE ID: **2026-81572**

CVSS 3.1 Score: 7.8
CVSS Vector: CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H

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