SECURITY ADVISORY

SPR-2506171, Issue 1

17 June 2025

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

Disclaimer: This document contains a general analysis and classification and is not tailored to the Customer's specific systems and configurations. The information and details are merely recommendations and therefore are to be applied by the Customer correspondingly to its own systems and configurations and implemented at its own discretion and under its own responsibility. No liability or guarantee for correctness or completeness is given.

CVE-2025-47809: Privilege Escalation through CodeMeter Installer on Windows

1. Summary

The CodeMeter Installer on Windows has a bug that allows under certain circumstances an Escalation of Privileges for an unprivileged account:
After installation on an Unprivileged Account with UAC using the built-in Administrator account, CodeMeter launches the CodeMeter Control Center with System privileges.

Sprecher Automation requires basic security hardening for SPRECON-V460 systems. Before installing any software, the basic hardening must be disabled. After installing the software, the basic hardening must be reactivated. Based on this, the following vulnerability classification was made.

2. Affected Products and Versions

SPRECON-V460 up to and including version 14 with CodeMeter Runtime < 8.30a installed.

3. Workarounds and Mitigations

SPRECON-V460 Systems are **not affected** and require **no remediation** if any of the following actions occurred after CodeMeter was installed:

1. The system was restarted
2. The user logged off
3. The CodeMeter Control Center was manually closed or restarted

Additionally, systems are **not impacted** in the following cases:

1. The user account belongs to the **Administrator group**
2. CodeMeter Runtime was installed using the parameter PROP_CMCC="none" or PROP_CMCC="auto", as both options prevent the CodeMeter Control Center from starting automatically after installation

Remedial measures: Install CodeMeter Runtime >= 8.30a.

4. Vulnerability Classification

CVSS 4.0 Score: 5.4
CVSS Vektor: AV:L/AC:L/AT:P/PR:H/UI:A/VC:H/VI:H/VA:H/SC:N/SI:N/SA: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. CVSS version 4.x is used in this document. 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

2025-06-17	Publication date