SECURITY ADVISORY SPRECON-V460 & SPRECON-TOOLS

SPR_SPRECON-V_2023-08, Issue 2

8 September 2023

Updates to the previous issue are marked in red

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 2023-3935: Heap buffer overflow in Wibu Systems CodeMeter Runtime can potentially lead to (remote) code execution

1. Summary

Sprecher Automation has been notified of a vulnerability in the Wibu Systems CodeMeter User Runtime Software that allows code execution via a buffer overflow, which is potentially exploitable over the network depending on the installation. The vulnerability has a CVSS 3.1 score of 9.0.

The CodeMeter User Runtime software is used by SPRECON-V460 for software license protection. The issue has been fixed by Wibu Systems and a new version 7.60c of the CodeMeter User Runtime Software is available which fixes the vulnerability. On existing SPRECON-V460 installations, this runtime can be replaced/updated without having to update/reinstall the V460 system.

In addition, the CodeMeter User Runtime is also used for licensing with SPRECON-Tools (SPRECON-E Service Program, SPRECON-E Designer, SPRECON-E PLC Designer, SPRECON-E Display Editor), but only if licensing is done via Wibu CodeMeter USB dongle and the SPRECON Licensing Driver Package is installed for this purpose.

2. Affected Products and Versions

Note: The CodeMeter User Runtime software can also be used by software products from other manufacturers. It should therefore be checked in any case whether this software is installed. CodeMeter User Runtime Software versions up to 7.60b are affected and should be updated.

2.1. SPRECON-V460

The CodeMeter User Runtime software is used for dongle and soft licensing of Engineering Studio/Editor, Service Engine/Runtime, Report Engine/Analyzer, Smart Server/Webserver, Logic Service/Logic Runtime, the Logic Studio/Logic Workbench and IIoT Services/ServiceGrid. The CodeMeter User Runtime software is part of the installation of these software products, even if no dongle licence is used.

- SPRECON-E V460 versions from 6.50 can be affected in principle. Versions higher than 8.00 only use the CodeMeter User Runtime Software from Wibu Systems and are definitely affected by this vulnerability.
- Versions up to and including 8.00 may use the CodeMeter User Runtime Software from Wibu Systems and could be affected by this vulnerability.
- All Reporting Engine/ Analyzer versions use the CodeMeter User Runtime software from Wibu Systems and are affected by this vulnerability.

2.2. SPRECON-Tools

The CodeMeter User Runtime is also used with SPRECON-Tools for dongle licensing (SPRECON-E Service Program, SPRECON-E Designer, SPRECON-E PLC Designer, SPRECON-E Display Editor). If one of these tools is licensed to a CodeMeter USB dongle, the SPRECON Licensing Driver Package must be installed for this purpose, which in turn installs the CodeMeter Runtime. All SPRECON Licensing Driver Packages up to and including 1.13 SP1 are affected by this vulnerability. Only with 1.13 SP2 the package provides the current CodeMeter Runtime 7.60c.

3. Workarounds and Mitigations

In a standard installation of SPRECON-V460 and also SPRECON Licensing Driver Package, the CodeMeter Runtime is not configured to act as a CodeMeter Runtime Server. In this case, the vulnerability only exists locally on the respective system, which reduces the CVSS Temporal Score to 7.1. The CodeMeter WebAdmin interface can be used to check whether it is a local installation or a runtime server.

If the CodeMeter Runtime is configured to act as a CodeMeter Runtime Server, CodeMeter licenses for SPRECON-V460 products are provided over the network, thus the vulnerability has a CVSS base score of 9.0 and is exploitable over the network.

Wibu Systems provides additional information with advisory WIBU-230704-01:
https://www.wibu.com/de/support/security-advisories.html

Sprecher Automation recommends updating the CodeMeter User Runtime - if existing - on the system. This is provided by the manufacturer in version 7.60c:
https://www.wibu.com/support/user/downloads-user-software.html

3.1. Workarounds

The following actions are recommended to reduce the risk until the corrected version can be installed. Please note that not all remedial measures apply to every possible product configuration. Therefore, check which of these measures might be relevant or applicable in your case.

- Restrict unprivileged access to machines running the CodeMeter User Runtime software to prevent local exploitation of the vulnerability.
- Configure the licence access rights in CodeMeter WebAdmin for the CodeMeter User Runtime Software and restrict access to the machines that require a licence from this CodeMeter Runtime Server.
- Enable HTTPS for the CodeMeter WebAdmin to ensure a secure connection to the configuration interface.
- Deny remote access to the CodeMeter WebAdmin if administration can be done locally.
- Configure authentication for read and write access for the CodeMeter WebAdmin to prevent unauthorised users from making changes.

3.2. Update Procedure

For existing installations with a CodeMeter licence, it is necessary to download the updated CodeMeter User Runtime Software for Windows from Wibu Systems and install this version on the affected systems to fix the vulnerability.

The installer of the CodeMeter User Runtime Software for Windows is able to update an existing installation. It is not necessary to uninstall the existing CodeMeter User Runtime Software for Windows.

Close all applications during the installation of the updated CodeMeter User Runtime Software for Windows.

Reboot the system to complete the update successfully.

If the CodeMeter licence is used as a local licence (most likely scenario) and not used as a network licence, it is not necessary to configure the CodeMeter Runtime as a CodeMeter Runtime Server.

The CodeMeter User Runtime software is compatible with current Windows versions.

4. Vulnerability Classification

CVE ID:	**2023-3935**
CVSS 3.1 Score:	9.0
CVSS Vector:	AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H
Description:	Heap buffer overflow in CodeMeter Runtime can potentially lead to (remote) code execution.

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 3.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

2023-08-23: Issue 1 Publication date
2023-09-08: Issue 2 Supplement SPRECON-Tools