09.09.2020

SPRECON-V460 SECURITY VULNERABILITY ANNOUNCEMENT 2020-09

Vulnerabilities in Wibu Systems CodeMeter Runtime Software

Sprecher Automation GmbH
Franckstraße 51, 4020 Linz / Österreich
Tel. +43 732 6908-0
Fax +43 732 6908-278
info@sprecher-automation.com
www.sprecher-automation.com

1. History

Date	Issue	Comment
09.09.2020	1	Created

2. Introduction

Sprecher Automation informs about detailing several severe and also critical security vulnerabilities in different versions of the Wibu Systems CodeMeter User Runtime software.

The CodeMeter User Runtime Software is used by SPRECON-V460 for its software license protection.

The issues were addressed by Wibu Systems and a new version 7.10 was made available by Wibu Systems, in which these issues were resolved.

The CodeMeter User Runtime software is used for dongle and soft licensing by the SPRECON-V460 Editor, SPRECON-V460 Runtime, SPRECON-V460 Analyzer, SPRECON-V460 Web Server, SPRECON-V460 Logic/Straton Runtime and the Logic/Straton Workbench. This software is part of the installation of these software products, even when no dongle license is used.

SPRECON-V460 versions 8.00 and higher exclusively use the CodeMeter User Runtime software from Wibu Systems and are affected by these vulnerabilities.
SPRECON-V460 versions 8.00 and lower may use the CodeMeter User Runtime software from Wibu Systems and might be affected by these vulnerabilities.
The SPRECON-V460 Analyzer exclusively uses the CodeMeter User Runtime software from Wibu Systems and is affected by these issues.

3. Affected components

- Systems where the SPRECON-V460 Editor, SPRECON-V460 Runtime, SPRECON-V460 Analyzer, SPRECON-V460 Web Server or SPRECON-V460 Logic/Straton Workbench have been installed may contain a version of the CodeMeter User Runtime software and might be affected by one or more of the reported vulnerabilities.

Note: The CodeMeter User Runtime software may also be used by software products from other vendors.

4. Affected versions

- CodeMeter User Runtime software versions 7.0 and lower are affected.
- SPRECON-V460 product versions 6.51 and newer are affected.

5. Vulnerability details

5.1. CVE-2020-14509

CodeMeter Runtime DoS due to Buffer Access with Incorrect Length Value.

CVSS v3 base score and vector:
A CVSS base score of **10.0** has been calculated for this vulnerability. The corresponding CVSS v3 vector:
AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H

Additional information:
The vulnerability is present on all systems with a vulnerable version of the CodeMeter User Runtime software installed. An attacker could send specially crafted packets that can result in a crash of the CodeMeter.exe and potentially allow code execution.

5.1.1. Mitigation

- Restrict (bind) the CodeMeter User Runtime software to the localhost only, to avoid exposure over the network. Only an update of the CodeMeter User Runtime software can fully resolve this vulnerability.

5.1.2. Remediation

- Update the CodeMeter User Runtime software to version 7.10 or higher

5.2. CVE-2020-14513

Improper Input Validation of WibuRaU files in CodeMeter Runtime.

CVSS v3 base score and vector:
A CVSS base score of **7.5** has been calculated for this vulnerability. The corresponding CVSS v3 vector:
AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H

Additional information:
The vulnerability is present on all systems with a vulnerable version of the CodeMeter User Runtime software installed. When the user executes a specially crafted license file, the CodeMeter User Runtime software may stop responding.

5.2.1. Mitigation

- Use RaU files from trusted sources only.

5.2.2. Remediation

- Update the CodeMeter User Runtime software to version 6.81 or higher.

5.3. CVE-2020-14515

Improper Signature Verification of CmActLicense update files for CmActLicense Firm Code.

CVSS v3 base score and vector:

A CVSS base score of **7.4** has been calculated for this vulnerability. The corresponding CVSS v3 vector: AV:L/AC:H/PR:N/UI:R/S:C/C:N/I:H/A:H

Additional information:

The vulnerability is present on all systems with a vulnerable version of the CodeMeter User Runtime software installed. An attacker may use manipulated CmActLicense files to modify existing licenses or build new licenses.

5.3.1. Mitigation

- -

5.3.2. Remediation

- Update the CodeMeter User Runtime software to version 6.90 or higher.

5.4. CVE-2020-14517

CodeMeter Runtime API: Inadequate Encryption Strength and Authentication.

CVSS v3 base score and vector:

A CVSS base score of **9.4** has been calculated for this vulnerability. The corresponding CVSS v3 vector: AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:H/A:H

Additional information:

The vulnerability is present on all systems with a vulnerable version of the CodeMeter Runtime installed.

5.4.1. Mitigation

- Restrict (bind) the CodeMeter User Runtime software to the localhost only to avoid exposure over the network.
- Restrict access to a CodeMeter User Runtime software running as a Server to trusted connections only.
- Only an update of the CodeMeter User Runtime software can fully resolve this vulnerability.

5.4.2. Remediation

- Update the CodeMeter User Runtime software to version 6.90 or higher.
- Update the CodeMeter User Runtime software to version 7.00b or higher when running the CodeMeter Runtime as Runtime Server.

5.5. CVE-2020-14519

CodeMeter Runtime WebSockets API: Missing Origin Validation.

CVSS v3 base score and vector:

A CVSS base score of **8.1** has been calculated for this vulnerability. The corresponding CVSS v3 vector: AV:N/AC:L/PR:N/UI:R/S:U/C:N/I:H/A:H

Additional information:

The vulnerability is present on all systems with a vulnerable version of the CodeMeter Runtime installed.

5.5.1. Mitigation

- Disable the CodeMeter Websockets API.

5.5.2. Remediation

- Update the CodeMeter User Runtime software to version 7.0 or higher and disable the Websockets API.

5.6. CVE-2020-16233

CodeMeter Runtime API: Heap Leak.

CVSS v3 base score and vector:

A CVSS base score of **7.5** has been calculated for this vulnerability. The corresponding CVSS v3 vector: AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N

Additional information:

The vulnerability is present on all systems with a vulnerable version of the CodeMeter User Runtime software installed.

5.6.1. Mitigation

- Restrict (bind) the CodeMeter User Runtime software to the localhost only, to avoid exposure over the network.

5.6.2. Remediation

- Update the CodeMeter User Runtime software to version 7.10 or higher.

6. Mitigation

See chapter 5 for mitigation options for each individual vulnerability.

7. Patch availability

Wibu Systems provides an updated version 7.10 of the CodeMeter User Runtime software, which addresses the reported vulnerabilities.
The “CodeMeter User Runtime for Windows” software can be downloaded via this link:
https://www.wibu.com/support/user/user-software.html

8. Installation, Update

Considering the criticality of the issues reported, Sprecher Automation follows the advice of Wibu Systems and recommends installing the update as soon as possible.

Sprecher Automation recommends testing the updated version of the CodeMeter User Runtime software in a test environment to verify a normal operation of the system according to project-specific configuration and hardware environment, prior to installing the patch in a production environment.

Sprecher Automation recommends that a contingency plan is in place to roll back the installation of the updated version in case of any unexpected issues with the production environment after the installation.

8.1. Update on availability of version 7.10a

A new version 7.10a of the CodeMeter User Runtime software will tentatively be made available by Wibu Systems, on 17.09.2020. While we recommend considering an update to version 7.10 now, you may also choose to wait for the availability of version 7.10a.

Wibu Systems states the following:
Q: What should I do in the meantime until the version 7.10a is available?
A: Most vulnerabilities have already been fixed in previous versions, e.g. 6.81 or 7.10, so the current version 7.10 contains measures to fix or mitigate all CVEs. The version 7.10a will implement further measures to eliminate the remaining risks. To our knowledge, none of the listed vulnerabilities have been actively used to date. The decision whether to update to version 7.10 now and then later to version 7.10a, or whether to take the risk for a week and then update directly to version 7.10a, is a decision you must make for yourself, taking into account your individual circumstances.”

8.1.1. Procedure

For existing installations using a CodeMeter License it is necessary to download the updated CodeMeter User Runtime software for Windows version from Wibu Systems and install this version on the affected systems in order to resolve the security vulnerabilities.

The installer of the CodeMeter User Runtime software for Windows is capable of updating an existing installation. It is not required to uninstall the existing CodeMeter User Runtime software for Windows first.

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

Unplug CodeMeter dongles prior to installing the updated CodeMeter User Runtime software for Windows.

If prompted, perform a restart of the system in order to complete the update successfully. A restart of the system, even if not prompted, is recommended.

When the CodeMeter License is used as a local license (most likely scenario) and not as a network license, it is not required to configure the CodeMeter Runtime as a CodeMeter Runtime Server.

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

8.2. Installation Media

For SPRECON-V460 versions 8.00 and newer, Sprecher Automation will be providing updated versions of the DVD (ISO-Image) on the Sprecher Automation website that include the updated version of the CodeMeter User Runtime software.
These DVD (ISO-Image) can be used for new installations.

Note regarding existing installations:
While updated installation media contain an updated version of the CodeMeter User Runtime software, the CodeMeter User Runtime software is only installed when no previous CodeMeter Runtime Software exists on the system.

Uninstalling and installing SPRECON-V460 again using the updated installation media will not result in an updated CodeMeter Runtime Software. In this case, either uninstall CodeMeter Runtime Software explicitly after uninstalling SPRECON-V460, or manually install the current CodeMeter Software version 7.10 or 7.10a (when available).

If any other software was installed before the installation of a SPRECON-V460 product that also makes use of the CodeMeter User Runtime software, the installation of SPRECON-V460 may not update the existing CodeMeter User Runtime software. In this case, a manual installation of the updated version is required.

Please contact your Sprecher Automation representative if you have any questions on updating or replacing your existing installation media.

9. General recommendations

Sprecher Automation generally recommends restricting local physical access to authorized people only.

Sprecher Automation further recommends using application whitelisting to restrict execution of applications to only those applications that are required for the operation of the system.

Sprecher Automation recommends testing the updated version of the SPRECON-V460 software in a test environment to verify normal operation of the system according to project specific configuration and hardware environment, prior to installing the update in a production environment.

Sprecher Automation recommends that a contingency plan is in place to roll back the installation of the update in case of any unexpected issues with the production environment following the installation of the patch.

Sprecher Automation generally recommends keeping the operating system and software up to date.

Sprecher Automation generally recommends using the SPRECON-V460 Editor on a separate engineering system in a protected environment to which access is restricted to authorized users only and on which appropriate security measures like the use of application whitelisting and antivirus software, are in place.