Security Vulnerability Announcement 2020_1

Vulnerabilities in Wibu Systems CodeMeter Runtime Software

www.copadata.com
sales@copadata.com

zenon
by COPA-DATA

1. History

Date	Comment
24.08.2020	Created
08.09.2020	Updated information on version 7.10a (see section 9.1)
12.10.2020	Updated Known Issues section Updated versions affected (from version 6.50)

Content

2. Introduction

COPA-DATA received a report from Wibu Systems detailing several severe and also critical security vulnerabilities in different versions of the CodeMeter User Runtime software.

The CodeMeter User Runtime Software is used by COPA-DATA products 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 zenon Editor, zenon Runtime, zenon Analyzer, zenon Web Server, zenon Logic Runtime and the straton Workbench. This software is part of the installation of these software products, even when no dongle license is used.

zenon versions 8.00 and higher exclusively use the CodeMeter User Runtime software from Wibu Systems and are affected by these vulnerabilities.

zenon versions 8.00 and lower may use the CodeMeter User Runtime software from Wibu Systems and might be affected by these vulnerabilities.

The zenon Analyzer exclusively uses the CodeMeter User Runtime software from Wibu Systems and is affected by these issues.

3. Products affected

Systems where the zenon Editor, zenon Runtime, zenon Analyzer, zenon Web Server, zenon logic Workbench, or 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. Versions affected

- CodeMeter User Runtime software versions 7.0 and lower are affected
- zenon product versions 6.50 and newer are affected

5. Vulnerability details

The report by Wibu Systems contains the following vulnerabilities. Details are provided for each individual vulnerability.

- CVE-2020-14509
- CVE-2020-14513
- CVE-2020-14515
- CVE-2020-14517
- CVE-2020-14519
- CVE-2020-16233

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.

Mitigations

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.

Remediation

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

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.

Mitigations

Use RaU files from trusted sources only.

Remediation

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

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.

Mitigations

-

Remediation

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

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.

Mitigations

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.

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.

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.

Mitigations

Disable the CodeMeter Websockets API.

Remediation

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

CVE-2020-16233:

CodeMeter Runtime API: Heap Leak

CVSS v3 base score and vector:

A CVSS base score of **7.5** was 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.

Mitigations

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

Remediation

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

6. 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/downloads-user-software.html

7. Known issues

Following an update of the CodeMeter User Runtime software, the settings in the Server Search List on systems where a network dongle is used may get lost. In such cases the hostname(s) / ip address(es) should be re-entered.

8. Mitigation

See section 5 for mitigation options for each individual vulnerability

9. Remediation

Recommendations

COPA-DATA recommends that asset owners and system integrators perform a risk assessment to identify whether the updated version of the CodeMeter User Runtime software shall be installed or not

Considering the criticality of the issues reported, COPA-DATA follows the advice of Wibu Systems and recommends installing the update as soon as possible.

COPA-DATA 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.

COPA-DATA 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.

9.1. 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."

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. (See Patch Availability for the link)

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.

10. Installation Media

For versions zenon 8.00 and newer, COPA-DATA will be providing updated versions of the .ISO and .BIN downloads on the COPA-DATA website that include the updated version of the

CodeMeter User Runtime software. These .ISO and .BIN files can be used for new installations.

COPA-DATA will be providing an up-to-date version of the USB drives with new licenses that include the updated version of the CodeMeter software, for versions 8.00 and higher.

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 zenon 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 zenon, or manually install the current CodeMeter Software version 6.50a.

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

Please contact your COPA-DATA representative if you have any questions on updating or replacing your existing installation media.

11. General recommendations

In general, COPA-DATA recommends restricting local physical access to authorized people only. Network communication shall be restricted to allow only those connections that are required.

Using VLANs and firewalls to segment network traffic and create zones and conduits reduces the exposure of vulnerable systems and allows access to a CodeMeter Runtime Server to be restricted to only those systems that are in fact using a network dongle. It is recommended that systems hosting a CodeMeter Runtime Server are not facing external networks.

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

12. Acknowledgements

COPA-DATA wishes to thank Wibu Systems for announcing the publication of these issues to their partners, prior to the public release.