Security Vulnerability Announcement 2021_2

Vulnerability in Wibu Systems CodeMeter Runtime Software

www.copadata.com
security@copadata.com

zenon
by COPA-DATA

1. History

Date	Comment
06.10.2021	Announcement Created
28.02.2022	Update regarding previous versions

Content

2. Introduction

COPA-DATA received a report from Wibu Systems detailing a severe security vulnerability 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 issue has been addressed by Wibu Systems and a new version 7.30a is available, in which this issue has been resolved.

The CodeMeter User Runtime software is used for dongle and soft licensing by the zenon Editor / Engineering Studio, zenon Runtime / Service Engine, zenon Analyzer / Report Engine, zenon Web Server / Smart Server, zenon Logic Runtime / Logic Service and the straton Workbench / Logic Studio. 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 / Reporting Engine exclusively uses the CodeMeter User Runtime software from Wibu Systems and is affected by these issues.

3. Products affected

Systems where the zenon Editor / Engineering Studio, zenon Runtime / Service Engine, zenon Analyzer / Reporting Engine, zenon Web Server / Smart Server, zenon logic Workbench / Logic Studio, 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

- All Windows versions of CodeMeter User Runtime software are affected
- zenon product versions 6.50 and newer are affected

5. Vulnerability details

The report by Wibu Systems contains the following vulnerability. Details are provided below.

- CVE-2021-41057

CVE-2021-41057:

CodeMeter Runtime for Windows: Denial of Service (DoS)

CVSS v3.1 base score and vector:

A CVSS base score of **7.1** has been calculated for this vulnerability.

The corresponding CVSS v3.1 vector:

https://www.first.org/cvss/calculator/3.1#CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:H/A:H

Additional information

If an attacker with basic user capabilities manages to set up a link to a special system file used with CmDongles, then essential files in the system could get overwritten.

Exploiting the vulnerability requires at least an unprivileged user account on the machine.

The mobile use of the CodeMeter Runtime is not affected by this vulnerability because in this case, CodeMeter runs in the user space instead of running as a Windows service.

Please note, that the mobile use of the CodeMeter Runtime is not used in conjunction with zenon products and allows using hardware dongles only.

Wibu Systems also provides additional information through the following link:

Security Advisories: Wibu-Systems

Mitigations

Following measures are recommended to reduce the risk until the fixed version can be installed. Please be aware that not all mitigations apply to every possible product configuration, so please check which of these could be relevant or applicable in your case.

- Restrict unprivileged access to machines running the CodeMeter License Server service.
- Disable the container type “Mass Storage” in CodeMeter: if there are no CmDongles connected to the affected machine or if the connected CmDongles are configured as HID, the CodeMeter communication with “Mass Storage” devices can be disabled at the Windows Registry as follows:
    - Set the value of the key “HKEY_LOCAL_MACHINE\SOFTWARE\WIBUSYSTEMS\CodeMeter\Server\CurrentVersion\EnabledContainerTypes” to 4294967294 (0xFFFFFFFE).
    - Restart CodeMeter to apply this change.

Please note that COPA-DATA CodeMeter hardware dongles are delivered with a HID configuration. When using additional CodeMeter Dongles for other applications, changing the registry key may disable the use of such dongles when these are in a mass storage configuration.

Remediation

Wibu Systems provides the CodeMeter User Runtime software version 7.30a that resolves the issue.

6. Patch Availability

Wibu Systems provides an updated version 7.30a of the CodeMeter User Runtime software, which addresses the reported vulnerability.

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

-

8. Mitigation

See section 5 for mitigation options for each individual vulnerability

9. Remediation

9.1. 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 issue reported, COPA-DATA follows the advice of Wibu Systems and recommends installing the update at the next opportunity.

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.

While compatibility of the CodeMeter Runtime Software version 7.30a has been validated explicitly with versions 8.20 and 10 of the zenon software platform, COPA-DATA has not recognized any incompatibilities with previous versions (8.10, 8.00 and older) and does not expect any.

9.2. Update 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 8.20 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 8.20 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 7.30a.

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.