

WIBU Systems CodeMeter Runtime Vulnerabilities in Vector Informatik GmbH Products

Vector Security Advisory

Version 1.4 of 2021-01-13

Author	Vector Informatik GmbH
Publisher	Vector Informatik GmbH © 2021 All rights reserved. Any distribution or copying is subject to prior written approval by Vector. Note: Hardcopy documents are not subject to change management.

Change History

Version	Date	Changes
1.0	01-10-2020	Final Version
1.1	09-10-2020	Chapter 3 Resolution for Vector Hardware Products updated
1.2	14-10-2020	Chapter 3 Resolution for Vector Hardware Products extended
1.3	15-10-2020	Chapter 2 Resolution of the Issue for PREEvision extended
1.4	13-01-2021	Chapter 3 Resolution for Vector Hardware Products extended

Contents

1 Summary	5
2 Resolution of the Issue for all Vector Software Products	6
2.1 Resolution of the Issue for PREEvision	6
2.1.1 If you are NOT using a Vector Keyman / CodeMeter Dongle (CmDongle)	6
2.1.2 If you are using a Vector Keyman / CodeMeter Dongle (CmDongle)	6
3 Resolution for Vector Hardware Products.....	7
4 General Security Recommendations	8
5 Contact	9

1 Summary

We inform you about a critical security vulnerability in a software component used in Vector products for licensing. Please note that the WIBU CodeMeter component is part of most Vector deliveries (Software and Hardware) and is also part of the Demo Versions that are available at www.vector.com.

In addition, the CodeMeter component can also be installed on your system via other manufacturers.

Vendor: WIBU-Systems AG

Component: CodeMeter

Reported Vulnerabilities: WIBU has reported six Vulnerabilities in all CodeMeter Versions earlier than CodeMeter 7.10a. This component is used by Vector for license management purposes. The vulnerabilities are identified as CVE-2020-14509, CVE-2020-14513, CVE-2020-14515, CVE-2020-14517, CVE-2020-14519, and CVE-2020-16233.

An attacker could use the vulnerabilities to alter and forge a license file, cause a denial-of-service condition, potentially attain remote code execution, read heap data, and prevent normal operation of third-party software dependent on the CodeMeter.

A detailed description of the vulnerabilities can be found on WIBU-Homepage:

<https://www.wibu.com/de/support/security-advisories.html>

2 Resolution of the Issue for all Vector Software Products

The vulnerabilities are resolved in CodeMeter 7.10a or higher.

Vector has verified CodeMeter 7.10a, for compatibility with Vector Products. We found no compatibility issues.

Hence, we strongly recommend an immediate update to CodeMeter 7.10a on all systems.

If possible, we recommend deploying the CodeMeter component (CodeMeter 7,10a) by your IT organization to all systems where a Vector product might have been installed in the past.

You can download the latest CodeMeter from WIBU-Systems' homepage:

<https://www.wibu.com/de/support/anwendersoftware/anwendersoftware.html>

Alternatively, you can download and install the latest Vector License Client (download from www.vector.com/vlc/). We have already integrated the latest CodeMeter, which will be installed along with Vector License Client.

2.1 Resolution of the Issue for PREEvision

PREEvision is using CodeMeter on your clients only if you are using a Hardware-Dongle, named Vector Keyman or CodeMeter Dongle. Due to the fact that we are delivering the CodeMeter software as part of the PREEvision client, we recommend the proposed solution in previous section.

2.1.1 If you are NOT using a Vector Keyman / CodeMeter Dongle (CmDongle)

We strongly recommend to update CodeMeter 7.10a on your system, if already installed.

Also, please remove the following files from your PREEvision installation:

<PREEvision_installation_path>\res\tools\wibu\CmDust.exe

<PREEvision_installation_path>\res\tools\wibu\CodeMeter.exe

<PREEvision_installation_path>\plugins\aquintos.commonresources...\res\wibu\v522a\cmu32.exe

<PREEvision_installation_path>\plugins\aquintos.commonresources...\res\wibu\v522a\CodeMeter.exe

<PREEvision_installation_path>\plugins\aquintos.core...\res\wibu\CmDust.exe

<PREEvision_installation_path>\plugins\aquintos.core...\res\wibu\cmu32.exe

<PREEvision_installation_path>\plugins\aquintos.core...\res\wibu\CodeMeter.exe

2.1.2 If you are using a Vector Keyman / CodeMeter Dongle (CmDongle)

We strongly recommend to newly install CodeMeter 7.10a on your system, even if not available.

Please do not delete the files listed in chapter 2.1.1 They will not be used during runtime but need to be available on the disk.

3 Resolution for Vector Hardware Products

This overview shows the recommended way how to solve the issue for Vector hardware products:

Product Group	Resolution
VT System	Update CodeMeter using Remote Desktop
CANoe RT Rack, VP Family, BRICK PCs	Update CodeMeter using Remote Desktop, or interactively directly on the device
VN89xx Family, VN88xx Family	Update CodeMeter using <u>Vector Driver Setup 11.6</u>
VN8910(A)	CodeMeter cannot be updated due to technical factors. Urgent recommendation: Use only in an environment cut off from the external network
All other Interfaces	CodeMeter Version 7.10a or higher https://www.wibu.com/de/support/anwendersoftware/anwendersoftware.html

Additional remarks:

- If Vector Products are connected via USB only, the vulnerabilities won't be exploited.
- Ensuring that the Vector Product (connected via Ethernet to the PC) is operating in a **protected environment** will prevent CodeMeter vulnerabilities from being exploited (<https://www.wibu.com/support/security-advisories.html>).
- Nevertheless, an update of CodeMeter is strongly recommended.

4 General Security Recommendations

We strongly recommend to install and use the latest version of CodeMeter but minimum version 7.10a immediately. If you cannot update your system immediately, we recommend other security measures.

5 Contact

Vector Informatik GmbH

www.vector.com/contact

support@vector.com