WIBU-100120: Privilege Escalation through CodeMeter Installer on Windows

Sharing rules

TLP:CLEAR
For the TLP version see: https://www.first.org/tlp/

Publishing Details

Publisher	WIBU-SYSTEMS AG
Webseite	https://www.wibu.com
Security Advisories	https://www.wibu.com/support/security-advisories.html

Document Details

Document Name	Privilege Escalation through CodeMeter Installer on Windows
Document version	1.1.0
Initial release date	2025-05-14T10:00:00.000Z
Current release date	2025-05-20T07:00:00.000Z
Language	en-US
Status	final
Also referred to	
Document category	csaf_security_advisory

Vulnerability Details

CVSSv3.1 Base Score(s)	7.7
CVSSv3.1 Vector(s)	CVSS:3.1/AV:L/AC:L/PR:H/UI:R/S:C/C:H/I:H/A:H
Maximal Severity	High

Vulnerability Title

The CodeMeter Installer on Windows has a bug that allows under certain circumstances an Escalation of Privileges for an unprivileged account: After installation on an Unprivileged Account with UAC using the built-in Administrator account, CodeMeter launches the CodeMeter Control Center with System privileges.

Vulnerabilities

Improper privilege dropping after installing CodeMeter Runtime on an unprivileged user account with User Access Control (UAC) in Windows allows privilege escallation on locally started CodeMeter Control Center. (CVE-2025-47809)

Description

After installing CodeMeter Runtime on Windows with the provided installer, the installer launches the CodeMeter Control Center directly, allowing the user to quickly start importing licences by using the provided system tray icon. If the user is unprivileged, UAC (https://support.microsoft.com/en-us/windows/user-account-control-settings-d5b2046b-dcb8-54eb-f732-059f321afe18) is activated and if the installation is authorized by the built-in Administrator account by having the admin type in his password, then the CodeMeter Control Center is launched once as administrator and will remain with these privileges until it is either manually closed or the user is logged out. Through the file selection dialog on "File" --> "Import License" and by then setting the files to "All files (.*)", a malicious user can navigate, for example, to C:\Windows\System32\ and right-click on cmd.exe and select "open", thus getting an administrator console. This vulnerability only affects freshly installed systems until CodeMeter Control Center is restarted.

Not affected: Systems are **not affected** and require **no remediation** if any of the following actions occurred after CodeMeter was installed:

1. The system was restarted
2. The user logged off
3. The CodeMeter Control Center was manually closed or restarted

Additionally, systems are **not impacted** in the following cases:

1. The user account belongs to the **Administrator group**
2. CodeMeter Runtime was installed using the parameter PROP_CMCC="none" or PROP_CMCC="auto", as both options prevent the CodeMeter Control Center from starting automatically after installation

CWE: CWE-269:Improper Privilege Management

Product status

Known affected

Product	CVSS-Vector	CVSS Base Score
CodeMeter Runtime < 8.30a	CVSS:3.1/AV:L/AC:L/PR:H/UI:R/S:C/C:H/I:H/A:H	7.7

Fixed

- CodeMeter Runtime >= 8.30a

Remediations

Vendor fix (2025-05-14T10:00:00.000Z)

For existing installations where the CodeMeter Control Center has been restarted at least once after installation, there is no action needed. Also, the "Reduced" Installer does not come with the CodeMeter Control Center and is therefore not affected.

For new installations, we recommend to install CodeMeter in Version 8.30a or higher for new installations.

If an earlier version of CodeMeter has to be installed, there are four options to mitigate the problem:

1. Do not use the built-in Administrator account for installation but a normal user account that is part of the Administrator group.

2. If using the built-in Administrator account for installation is inevitable, manually terminate the CodeMeter Control Center (via File --> Exit or by pressing CTRL+Q) after installation and restart as

the current user. Please note that closing the window using ALT+F4 or the close button does not suffice, as the CodeMeter Control Center still runs in the background.

3. Ending the session (either by log-out or rebooting Windows) after the installation solves the issue: Starting a new session launches the CodeMeter Control Center with user privileges.

4. Use the installation parameter PROP_CMCC=""none"" or PROP_CMCC=""auto"" to prevent the start of CodeMeter Control Center at the end of the installation. Note: PROP_CMCC=""none"" additionally disables the CodeMeter Control Center entry in the auto start directory. For more technical details please go to the CodeMeter Developer Guide, section: "Deploying on Windows Operating Systems" > "Customizing Options for Installation Packages".

For products:

- CodeMeter Runtime < 8.30a

Acknowledgments

- Mateusz Gierblinski for reporting this vulnerability and helping us to reconstruct it following a coordinated disclosure.

WIBU-SYSTEMS AG

Namespace: https://wibu.com

cert@wibu.com

WIBU-CERT

Revision history

Version	Date of the revision	Summary of the revision
1.0.0	2025-05-14T10:00:00.000Z	First version, TLP:CLEAR
1.1.0	2025-05-20T07:00:00.000Z	Added: not affected configuration and a mitigation

Disclaimer

The information in this document is subject to change without notice and should not be construed as a commitment by WIBU-SYSTEMS AG. All information that relates to the future (e.g. planned software versions and release dates) is provided without guarantee. WIBU-SYSTEMS AG provides no warranty, express or implied, including warranties of merchantability and fitness for a particular purpose, for the information contained in this document, and assumes no responsibility for any errors that may appear in this document. In no event shall WIBU-SYSTEMS AG or any of its suppliers be liable for direct, indirect, special, incidental, or consequential damages of any nature or kind arising from the use of this document, or from the use of any hardware or software described in this document, even if WIBU-SYSTEMS AG or its suppliers have been advised of the possibility of such damages. This document and parts hereof must not be reproduced or copied without written permission from WIBU-SYSTEMS AG, and the contents hereof must not be imparted to a third party nor used for any unauthorized purpose. All rights to registrations and trademarks reside with their respective owners.

Sharing rules

TLP:CLEAR
For the TLP version see: https://www.first.org/tlp/