SECURITY
LICENSING
PERFECTION IN PROTECTION

WIBU
SYSTEMS

2021-10-04
Version 1.2

Security Advisory WIBU-210910-01

Vulnerability title

CodeMeter Runtime for Windows: Denial of Service (DoS)

Vulnerability description

A local attacker could cause a Denial of Service by overwriting existing files on the affected system.

- CVE: CVE-2021-41057
- CVSS v3.1 base score: 7.1
- CVSS v3.1 vector string: /AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:H/A:H
- Vulnerability type: CWE-269

Vulnerability details

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.

Affected products

Product name	Affected versions	Fixed versions
CodeMeter Runtime	All Windows versions	7.30a

Mitigations for affected versions

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\WIBU-SYSTEMS\CodeMeter\Server\CurrentVersion\EnabledContainerTypes” to 4294967294 (0xFFFFFFFE).
    - Restart CodeMeter to apply this change.

General security best practices can help to protect systems from local and network attacks.

Acknowledgments

We thank Jokūbas Arsoba for reporting this vulnerability following coordinated disclosure.

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.

Document History

Version	Date	Description
1.0	2021-09-29	Draft version, TLP:AMBER
1.1	2021-09-30	Integrated review feedback
1.2	2021-10-04	One mitigation was changed