

Product Security Advisory: WIBU-103081

Sharing rules



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

Vulnerability Title

Local Privilege Escalation in CodeMeter Runtime on Windows

Affected Products

Affected Products

CodeMeter Runtime 8.x versions 8.40 - 8.41
CodeMeter Runtime 9.x versions < 9.10

Fixed Products

CodeMeter Runtime 8.x versions >= 8.41a
CodeMeter Runtime 9.x versions >= 9.10

Vulnerability Details

Highest CVSSv3.1 Base Score	7.8
CVSSv3.1 Vector(s)	CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H
Highest Severity	High

Vulnerabilities

Local Privilege Escalation in CodeMeter Runtime on Windows (CVE-2026-81572)

Description

cmu.exe --create-io --file C: creates a predictable temporary file under C:\CM-Stick. The directory and file paths are not properly checked for NTFS reparse points, such as junctions or symbolic links, before file operations are performed. A local attacker can create a junction at the temporary file that points to an arbitrary system path. Because CodeMeter Runtime runs with System privileges, this could allow arbitrary files to be deleted with System privileges and potentially enable local privilege escalation.

CWE: CWE-59:Improper Link Resolution Before File Access ('Link Following')

Product status

Known affected

Product	CVSS-Vector	CVSS Base Score
CodeMeter Runtime 8.x versions 8.40 - 8.41	CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H	7.8
CodeMeter Runtime 9.x versions < 9.10	CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H	7.8

Fixed

- CodeMeter Runtime 8.x versions >= 8.41a
- CodeMeter Runtime 9.x versions >= 9.10

Acknowledgments

- Andreas Vikerup of Shelltrail AB

WIBU-SYSTEMS AG

WIBU-SYSTEMS CERT
Zimmerstrasse 5
D-76137 Karlsruhe

Namespace: <https://wibu.com>

cert@wibu.com

References

- Blog post by Shelltrail AB: <https://shelltrail.com/research/local-privilege-escalation-to-system-in-wibu-systems-codemeter-application>

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 WIBU-103081
Document version 1.1.1
Initial release date 2026-07-20T12:00:00.000Z
Current release date 2026-08-27T12:00:00.000Z
Language en-US
Status final

Also referred to

Document category csaf_security_advisory

Revision history

Version	Date of the revision	Summary of the revision
1.0.0	2026-07-20T12:00:00.000Z	Initial Version
1.1.0	2026-08-25T09:00:00.000Z	First public version
1.1.1	2026-08-27T12:00:00.000Z	Added CVE-IDs

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/>