SECURITY
LICENSING
PERFECTION IN PROTECTION

WIBU
SYSTEMS

2020-09-04
Version 1.1

# Security Advisory WIBU-200521-03

## Vulnerability Title

CodeMeter Runtime DoS due to Buffer Access with Incorrect Length Value

## Vulnerability description

Multiple memory corruption vulnerabilities exist where the packet parser mechanism of CodeMeter does not verify length fields. An attacker could send specially crafted packets to exploit these vulnerabilities.

- CVE: CVE-2020-14509
- CVSS v3.1 base score: 10.0
- CVSS v3.1 vector string: AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H
- Vulnerability type: CWE-805

## Vulnerability details

Sending malicious TCP/IP packets via local or remote network connections to CodeMeter.exe can cause a crash of CodeMeter.exe due to improper length value checks. Also a heap buffer overflow may occur, which could enable a remote code execution attack.

## Affected products

| Product name | Affected versions | Fixed versions |
|---|---|---|
| CodeMeter Runtime | All versions prior to 7.10a | CodeMeter Runtime 7.10a or newer. |

## Mitigation for affected versions

- Run CodeMeter as client only and use localhost as binding for the CodeMeter communication which is already the default configuration since CodeMeter Runtime 6.90. With binding to localhost an attack is no longer possible via remote network connection.
- If CodeMeter Runtime is required to run as network server use the CodeMeter License Access Permissions feature to restrict the usage of CodeMeter API.

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

## Acknowledgments

We thank Sharon Brizinov and Tal Keren of Claroty 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.

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.

## Document History

| Version | Date | Description |
|---|---|---|
| 1.0 | 2020-08-14 | Draft version |
| 1.1 | 2020-09-04 | Final Version |