SECURITY
LICENSING
PERFECTION IN PROTECTION

2020-09-04
Version 1.1

Security Advisory WIBU-200521-04

Vulnerability Title

CodeMeter Runtime API: Inadequate Encryption Strength and Authentication

Vulnerability description

Protocol encryption can be broken and the server accepts external connections, which may allow an attacker to remotely communicate with the CodeMeter API.

- CVE: CVE-2020-14517
- CVSS v3.1 base score: 9.4
- CVSS v3.1 vector string: AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:H/A:H
- Vulnerability type: CWE-326

Vulnerability details

This is related to the communication with the CodeMeter service if the CodeMeter API is used. The CodeMeter Runtime API Protocol does not support authentication and the encryption can be broken. This allows an attacker to execute any CodeMeter API remotely, if the CodeMeter Runtime is running as server. There is no possibility to securely store a secret on the client side to improve the encryption of the public CodeMeter API.

Affected products

Product name	Affected versions	Fixed versions
CodeMeter Runtime	All versions	See mitigations

Mitigation for affected versions

- Use CodeMeter Runtime 7.10a.
  This will remove the remote attack vector.
- For versions prior to 7.10a run CodeMeter as client only and use localhost as binding for the CodeMeter communication. 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