

2020-09-04

Version 1.1

Security Advisory WIBU-200521-05

Vulnerability Title

CodeMeter Runtime API: Heap Leak

Vulnerability description

An attacker could send a specially crafted packet that could have the server send back packets containing data from the heap.

- CVE: CVE-2020-16233
- CVSS v3.1 base score: 7.5
- CVSS v3.1 vector string: [AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N](#)
- Vulnerability type: CWE-404

Vulnerability details

CodeMeter Runtime returns data from the heap if an attacker is sending specially crafted TCP/IP packets (CodeMeter API Commands) to CodeMeter.exe.

Affected products

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

Mitigation for affected versions

- Run CodeMeter as client only and use localhost as binding for the CodeMeter communication.
This is already the default configuration since CodeMeter Runtime 6.90.
- 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