2021-06-10
Version 1.3

Security Advisory WIBU-210423-01

Vulnerability Title

CodeMeter Runtime Network Server: Heap Leak and Denial of Service

Vulnerability description

An attacker could send a specially crafted packet that could have the CodeMeter Runtime Network Server send back packets containing data from the heap or crash the server.

- CVE: CVE-2021-20093
- CVSS v3.1 base score: 9.1
- CVSS v3.1 vector string: AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:H
- Vulnerability type: CWE-126

Vulnerability details

An attacker could send a specially crafted TCP/IP packet that causes the CodeMeter Runtime network server (default port 22350) to return packets containing data from the heap. When generating a response, the server copies data from a heap-based buffer to an output buffer to be sent in the response. The amount to copy is controlled by the client. An unauthenticated remote attacker can exploit this issue to disclose heap memory contents or crash the CodeMeter Runtime Server (i.e., CodeMeter.exe).

Affected products

Product name	Affected versions	Fixed versions
CodeMeter Runtime	All versions	7.21a

Mitigation for affected versions

- 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. The network server is disabled by default.
- If it is not possible to disable the network server, using a host-based firewall to restrict access to the CmLAN port can reduce the risk.

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

Acknowledgments

We thank Tenable, Inc. 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	2021-04-29	TLP:RED draft
1.1	2021-05-06	Integrated review feedback
1.2	2021-06-09	TLP:AMBER with restriction
1.3	2021-06-10	Final public version