2023-10-19
Version v3.1

Product Security Advisory WIBU-230704-01

Vulnerability Title

Heap Buffer Overflow Vulnerability in CodeMeter Runtime

Affected products

Product name	Affected versions	Fixed Versions
CodeMeter Runtime	<7.60c All platforms	>=7.60c 7.21g

Vulnerability description

In CodeMeter Runtime versions up to 7.60b, there is a heap buffer overflow vulnerability which can potentially lead to a remote code execution. Currently, no PoC is known to us. To exploit the heap overflow, additional protection mechanisms need to be broken. Remote access is only possible if CodeMeter is configured as a server. If CodeMeter is not configured as a server, the adversary would need to log in to the machine where the CodeMeter Runtime is running or trick the user into sending a malicious request to CodeMeter. This might result in an escalation of privilege.

- CVE: CVE-2023-3935
- Network Server (base)
  - CVSS v3.1 base score: 9.0 (Critical)
  - CVSS v3.1 vector string: CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:C/C:H/I:H/A:H
- Network Server (temporal)
  - CVSS v3.1 base score: 7.8 (High)
  - CVSS v3.1 vector string: CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:C/C:H/I:H/A:H/E:U/RL:O/RC:C
- No Network Server (base)
  - CVSS v3.1 base score: 8.1 (High)
  - CVSS v3.1 vector string: CVSS:3.1/AV:L/AC:H/PR:N/UI:N/S:C/C:H/I:H/A:H
- No Network Server (temporal)
  - CVSS v3.1 base score: 7.1 (High)
  - CVSS v3.1 vector string: CVSS:3.1/AV:L/AC:H/PR:N/UI:N/S:C/C:H/I:H/A:H/E:U/RL:O/RC:C

- CWEs[1]:
  - CWE-122: Heap-based Buffer Overflow
  - CWE-20: Improper Input Validation

Remediation

- Installation of runtime version 7.60c or later

[1] Common Weakness Enumeration (CWE): https://cwe.mitre.org

Mitigations for affected versions

If possible, run CodeMeter as client only. Otherwise restrict access to server to required clients only by implementing an access list.

CodeMeter API is a privileged API, so please consider the corresponding recommendations when using privileged APIs, e.g. https://cwe.mitre.org/data/definitions/648.html, so that your application isn't affected by CWE-648 (Incorrect use of privileged APIs) or other related weaknesses.

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

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
3.0	2023-08-16	First version, TLP:CLEAR
3.1	2023-10-19	CWE-648 was listed in the wrong section of the security advisory, so it was moved to the "Mitigations" section. CodeMeter Runtime is not affected by CWE-648.