KRONES AG
Böhmerwaldstraße 5
93073 Neutraubling

KRONES Security Advisory “WIBU-SYSTEMS CodeMeter Runtime vulnerabilities, June 2021” (KSA-2021-5)

In June 2021, the WIBU-SYSTEMS AG published two security advisories regarding their license manager CodeMeter Runtime. Various software products of different vendors rely on CodeMeter. An attacker, who successfully exploits the vulnerabilities, can crash the CodeMeter Runtime or read data from the heap on affected systems.

For the affected products and services, Krones rates the likelihood of being exploited as medium. Therefore, timely action is recommended.

Affected products and services

The following table lists affected products or services, and specific remediation. Krones recommends implementing the suggested remediation measures.

No.	Likelihood of exploitation[1]	Affected products or services	Default state and remediation
1	Medium	HMI systems based on Windows Embedded Standard 7 with image version: • IDC 4.xx • INS 1.xx • IPS 1.xx • IRS 1.xx • SAM 1.xx • PGD 1.xx (These HMI systems are based on zenon by COPA-DATA that uses the vulnerable CodeMeter Runtime.)	• We recommend implementing the mitigations listed below. • Krones may offer customer-specific updates. Please get in touch with Krones LCS.
2	Medium	HMI systems based on Windows 10 IoT with image version BBZ x.xx (These HMI systems are based on zenon by COPA-DATA that uses the vulnerable CodeMeter Runtime.)	• We recommend implementing the mitigations listed below. • Krones may offer customer-specific updates. Please get in touch with Krones LCS.
Krones may add additional affected products or services, or update remediations as soon as there is new information available.			

Workarounds and mitigations

The following specific workarounds and mitigations are recommended in addition to the remediation measures listed above to further reduce the risk originating from the security vulnerabilities:

- Use firewalls to block TCP and UDP traffic to ports 22350, 22351, and 22352 (used by the CodeMeter Runtime). The communication to this port is only needed on the localhost.

[1] The likelihood of exploitation is rated by Krones for the default Krones use case of the product in its delivery condition. This value may vary in case of customer-specific solutions or changes of the delivery condition.

- If applicable, monitor your complete network traffic to detect traffic to TCP and UDP ports 22350, 22351, and 22352.

Security contact

If you have any questions regarding this security advisory or other security-related questions, please contact the Product Security Incident Response Team (PSIRT) of Krones: cyber.security@krones.com

OpenPGP key for confidential messages:
https://www.krones.com/ext/securitytxt/cyber.security@krones.com.asc

Appendix A: Technical description of the vulnerabilities

This section describes each vulnerability in detail. The CVSS v3.1 base score is the current severity rating according to the original security advisories by WIBU-SYSTEMS and does not necessarily reflect the actual severity in the default Krones environment.

Vulnerability CVE-2021-20093

The CodeMeter Runtime Network Server allows a buffer over-read in the heap, which can be exploited to crash the CodeMeter Runtime or read sensitive data. The vulnerability affects all CodeMeter Runtime versions prior to 7.21a.

The CVSS v3.1 base score for the vulnerability is 9.1 (AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:H).

Vulnerability CVE-2021-20094

The CodeMeter Runtime crashes when processing a specially crafted HTTP request. In order to be exploited, the CodeMeter Runtime CmWAN server must be enabled, which is disabled by default. The vulnerability affects all CodeMeter Runtime versions prior to 7.21a.

The CVSS v3.1 base score for the vulnerability is 7.5 (AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H).

Appendix B: Further information

- Original security advisories by WIBU-SYSTEMS - https://www.wibu.com/support/security-advisories.html
- CISA “ICS Advisory (ICSA-21-210-02)” - Wibu-Systems CodeMeter Runtime | CISA
- COPA-DATA “Security Vulnerability Announcement 2021_1 - Vulnerabilities in Wibu Systems CodeMeter Runtime Software” - CD_SVA_2021_1.pdf (copadata.com)

Appendix C: Changelog

Version	Date	Changes
1.0	2021-08-02	Initial publication by the Krones PSIRT