KRONES AG
Böhmerwaldstraße 5
93073 Neutraubling

# KRONES Security Advisory “WIBU-SYSTEMS CodeMeter Runtime vulnerabilities, September 2020” (KSA-2020-3)

In September 2020, the WIBU-SYSTEMS AG published six 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 modify license files, cause denial-of-service conditions, read specific data, and may be able to remotely execute code 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:<br>• IDC 4.xx<br>• INS 1.xx<br>• IPS 1.xx<br>• IRS 1.xx<br>• SAM 1.xx<br>• PGD 1.xx<br>(These HMI systems are based on zenon by COPA-DATA that uses the vulnerable CodeMeter Runtime.) | • We recommend implementing the mitigations listed below.<br>• 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<br>(These HMI systems are based on zenon by COPA-DATA that uses the vulnerable CodeMeter Runtime.) | • We recommend implementing the mitigations listed below.<br>• 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-2020-14509

The CodeMeter Runtime is vulnerable to multiple buffer overflows that can result in crashes (denial of service) or remote code execution. The vulnerability affects all CodeMeter Runtime versions prior to 7.10a.

The CVSS v3.1 base score for the vulnerability is 10.0 (AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H).

### Vulnerability CVE-2020-14513

The CodeMeter Runtime doesn't respond anymore (denial of service) if a specifically crafted Update File (.WibuCmRaU) is provided. The vulnerability affects all CodeMeter Runtime versions prior to 6.81.

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).

### Vulnerability CVE-2020-14515

The CodeMeter Runtime accepts arbitrary license files (CmActLicense Update Files with CmActLicense Firm Codes). The vulnerability affects all CodeMeter Runtime versions prior to 6.90.

The CVSS v3.1 base score for the vulnerability is 7.4 (AV:L/AC:H/PR:N/UI:R/S:C/C:N/I:H/A:H).

### Vulnerability CVE-2020-14517

The CodeMeter API can be exploited when running as a server due to missing authentication and weak cryptography. Exploiting the vulnerability may lead to remote execution of commands supported by the API. The vulnerability affects all CodeMeter Runtime versions prior to 7.10a.

The CVSS v3.1 base score for the vulnerability is 9.4 (AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:H/A:H).

### Vulnerability CVE-2020-14519

The CodeMeter Runtime WebSockets API can be exploited with specifically crafted JavaScript to modify license files. If combined with CVE-2020-14515, license files can also be created. The vulnerability affects all CodeMeter Runtime versions prior to 7.10a.

The CVSS v3.1 base score for the vulnerability is 8.1 (AV:N/AC:L/PR:N/UI:R/S:U/C:N/I:H/A:H).

### Vulnerability CVE-2020-16233

The CodeMeter API can be exploited when running as a server to read data from the heap. The vulnerability affects all CodeMeter Runtime versions prior to 7.10.

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

KRONES AG
Böhmerwaldstraße 5
93073 Neutraubling

## Appendix B: Further information

- Original security advisories by WIBU-SYSTEMS - https://www.wibu.com/support/security-advisories.html
- CISA "ICS Advisory (ICSA-20-203-01)" - https://us-cert.cisa.gov/ics/advisories/icsa-20-203-01
- COPA-DATA "Security Vulnerability Announcement 2020_1 - Vulnerabilities in Wibu Systems CodeMeter Runtime Software" - https://www.copadata.com/fileadmin/user_upload/faq/files/CD_SVA_2020_1.pdf

## Appendix C: Changelog

| Version | Date | Changes |
|---|---|---|
| 1.0 | 2020-09-28 | Initial publication by the Krones PSIRT |
| 1.1 | 2020-10-21 | Added information regarding updated image versions that aren't affected |
| 1.2 | 2020-10-28 | Added information regarding new images, updated the text for CodeMeter on updated image versions |
| 1.3 | 2020-12-03 | Removed the updated image versions since alternative remediations are investigated |
| 1.4 | 2021-08-02 | Added information regarding customer-specific updates, added Windows 10 IoT based HMI with image version BBZ x.xx |