Manufacturer Information “CodeMeter”

The licensing of custo diagnostic 4.x is managed by the software protection system “CodeMeter” offered by WIBU-SYSTEMS AG.

WIBU-SYSTEMS AG has reported security weaknesses:

- CVE-2021-20093: CodeMeter Runtime Network Server: Heap Leak and Denial of Service
  This CVE vulnerability severity rating is 'Critical' (CVSS Score: 9.1).
  The vulnerability affects the TCP/IP communication of CodeMeter License Server. Sending manipulated packets can cause CodeMeter License Server to crash or read data from heap memory.
- CVE-2021-20094: CodeMeter Runtime CmWAN Server: Denial of Service (DoS)
  This CVE vulnerability severity rating is 'High' (CVSS Score: 7.5). The vulnerability affects communication with the CodeMeter CmWAN server. Sending special HTTP(S) requests to the CmWAN server can cause the CodeMeter License Server to crash. The CmWAN server is disabled by default.

A detailed overview of the vulnerabilities can be found in the corresponding Security Advisories, which you can download at https://wibu.com/support/security-advisories.html.

Generally, the operation of custo diagnostic takes place in closed medical networks, which cannot be accessed by external parties. In case your router, firewall, and the computers are protected sufficiently, the risk can be considered moderate.

WIBU-SYSTEMS AG made available an update for remedial action (Version CodeMeter 7.21a User Runtime) under the following link https://www.wibu.com/support/user/user-software.html.

In case of an update, all computers, on which custo diagnostic 4.x is installed (including PC with CodeMeter dongle), must be updated. This can be done by the user, or contact your regional custo med distributor. Generally, the operation can be done remotely.

06/2021

custo med GmbH
85521 Ottobrunn