# Security Advisory
## WIBU Systems CodeMeter Runtime Vulnerabilities in Rexroth Products

## 1 Advisory Information

**Advisory ID:** BOSCH-SA-231483
**CVE Numbers and CVSS v3.1 Scores:**

- CVE-2020-14513
  - Base Score: 7.5 (High)
- CVE-2020-14519
  - Base Score: 8.1 (High)
- CVE-2020-14509
  - Base Score: 10.0 (Critical)
- CVE-2020-14517
  - Base Score: 9.4 (Critical)
- CVE-2020-16233
  - Base Score: 7.5 (High)
- CVE-2020-14515
  - Base Score: 7.4 (High)

**Published:** 25 Sep 2020
**Last Updated:** 25 Sep 2020

## 2 Summary

A set of 6 vulnerabilities affect multiple versions of the WIBU Systems CodeMeter Runtime Software. This software is used by multiple Rexroth Products and Bosch Rexroth customers for license management. In order to successfully exploit these vulnerabilities, an attacker requires access to the network or system. One vulnerability (CVE-2020-14509) is notably critical, as it can easily be exploited by crafting packets sent over any network. The successful exploitation of these vulnerabilities can lead to DoS (CVE-2020-14513, CVE-2020-14509), remote code execution (CVE-2020-14509), bypassed encryption (CVE-2020-14517), heap leak on the licensing server-side (CVE-2020-16233) and manipulation or forgery of license files (CVE-2020-14519, CVE-2020-14515).

Bosch Rexroth recommends to update vulnerable components using the CodeMeter Runtime to version 7.10a. These vulnerabilities do not affect the CodeMeter Embedded Software.

## 3 Affected Products

- Rexroth ActiveAssist Tool localization extension module < 1.1
- Rexroth Laser Localization Software < 1.2

# 4 Solution

## 4.1 Software Update

It is strongly recommended that customers update the WIBU Systems CodeMeter Runtime Software hosted in their machines to version 7.10a . If an update is not possible in a timely manner, two mitigation approaches can be followed. The first is to employ Rexroth Products and their Licensing functions within a closed and/or secure network environment (as described below). The second mitigation alternative is to deactivate access to the WebSocket API (this must be performed on the licensing server-side).

### 4.1.1 Laser Localization Software

A new version of the Laser Localization Software (i.e. Laser Localization Software version 1.2) is expected to be available in October 2020. It is recommended that all instances using prior versions are updated to this software version once it is made available.

### 4.1.2 ActiveAssist

A new version 1.1 of the installation package for the extension module Tool localization of ActiveAssist is available as of September 24, 2020. It is recommended to update prior versions. The new version is readily available for registered customers as prior versions here on myRexroth.

## 4.2 Closed Network

Bosch Rexroth strongly recommends to operate the Laser Localization Software, ActiveAssist as well as the CodeMeter License Server host machine in a closed network with limited access to the system. Another alternative is to restrict the functions of the CodeMeter Runtime software by binding its communication to the localhost.

# 5 Vulnerability Details

## 5.1 CVE-2020-14513

Vulnerability: Improper input validation of update files in CodeMeter Runtime. Length checks are not properly executed.

Impact: A specially crafted license file may cause a crash in the CodeMeter and the software using it.

CVE description: CodeMeter (All versions prior to 6.81) and the software using it may crash while processing a specifically crafted license file due to unverified length fields.

- Problem Type:
  - IMPROPER INPUT VALIDATION CWE-20
- CVSS Vector String: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H
  - Base Score: 7.5 (High)

## 5.2 CVE-2020-14519

Vulnerability: No authentication and origin validation for connections using the CodeMeter Runtime WebSockets API.

Impact: Unauthorized reading of license information, dongle information and CodeMeter version, and update of licenses.

CVE description: This vulnerability allows an attacker to use the internal WebSockets API for CodeMeter (All versions prior to 7.00 are affected, including Version 7.0 or newer with the affected WebSockets API still

enabled. This is especially relevant for systems or devices where a web browser is used to access a web server) via a specifically crafted Java Script payload, which may allow alteration or creation of license files for when combined with CVE-2020-14515.

- Problem Type:
  - ORIGIN VALIDATION ERROR CWE-346
- CVSS Vector String: CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:N/I:H/A:H
  - Base Score: 8.1 (High)

## 5.3 CVE-2020-14509

Vulnerability: CodeMeter Runtime DoS due to Buffer Access with Incorrect Length Value.

Impact: A specially crafted TCP/IP packet may cause CodeMeter to crash. It may also cause a buffer overflow which could enable remote code execution.

CVE description: Multiple memory corruption vulnerabilities exist in CodeMeter (All versions prior to 7.10) where the packet parser mechanism does not verify length fields. An attacker could send specially crafted packets to exploit these vulnerabilities.

- Problem Type:
  - BUFFER ACCESS WITH INCORRECT LENGTH VALUE CWE-805
- CVSS Vector String: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H
  - Base Score: 10.0 (Critical)

## 5.4 CVE-2020-14517

Vulnerability: Protocol encryption can be broken when using the CodeMeter API, which may allow servers to accept external connections.

Impact: Servers may allow remote connections that can execute any CodeMeter API call.

CVE description: Protocol encryption can be easily broken for CodeMeter (All versions prior to 6.90 are affected, including Version 6.90 or newer only if CodeMeter Runtime is running as server) and the server accepts external connections, which may allow an attacker to remotely communicate with the CodeMeter API.

- Problem Type:
  - INADEQUATE ENCRYPTION STRENGTH CWE-326
- CVSS Vector String: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:H/A:H
  - Base Score: 9.4 (Critical)

## 5.5 CVE-2020-16233

Vulnerability: Heap Leak when using the CodeMeter Runtime API.

Impact: A specially crafted TCP/IP packet may cause a server to return heap data.

CVE description: An attacker could send a specially crafted packet that could have CodeMeter (All versions prior to 7.10) send back packets containing data from the heap.

- Problem Type:
  - IMPROPER RESOURCE SHUTDOWN OR RELEASE CWE-404
- CVSS Vector String: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N
  - Base Score: 7.5 (High)

### 5.6 CVE-2020-14515

Vulnerability: Signature verification issue when checking license file signatures. Only CmActLicense Update Files with CmActLicense Firm Codes are affected.

Impact: A specially crafted license file may be accepted as a valid license.

CVE description: CodeMeter (All versions prior to 6.90 when using CmActLicense update files with CmActLicense Firm Code) has an issue in the license-file signature checking mechanism, which allows attackers to build arbitrary license files, including forging a valid license file as if it were a valid license file of an existing vendor. Only CmActLicense update files with CmActLicense Firm Code are affected.

- Problem Type:
  - IMPROPER VERIFICATION OF CRYPTOGRAPHIC SIGNATURE CWE-347
- CVSS Vector String: CVSS:3.1/AV:L/AC:H/PR:N/UI:R/S:C/C:N/I:H/A:H
  - Base Score: 7.4 (High)

## 6 Additional Resources

[1] WIBU Systems Security Advisory page: https://www.wibu.com/support/security-advisories.html

## 7 Revision History

25 Sep 2020: Initial Publication