

04 August 2021  
300518567

## Security Advisory for PHOENIX CONTACT products utilizing WIBU SYSTEMS CodeMeter components

### Advisory Title

Denial of Service vulnerabilities in WIBU SYSTEMS CodeMeter

### Advisory ID

CVE-2021-20093  
CVE-2021-20094  
VDE-2021-036

### Vulnerability Description

**CVE-2021-20093:** CodeMeter Runtime Network Server: Heap Leak and Denial of Service  
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 (CWE-126).

**CVE-2021-20094:** CodeMeter Runtime CmWAN Server: Denial of Service (DoS)  
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 (CWE-126).

### **Affected products**

Article no	Article	Affected versions
--	Activation Wizard	1.4 and earlier
1046008	PC Worx Engineer	2021.06 and earlier
1165889	PLCNEXT ENGINEER EDU LIC (License codes)	2021.06 and earlier
2702889	FL Network Manager	5.0 and earlier
1153509,1153513, 1086929,1153516, 1086891,1153508, 1153520,1086921, 1086889,1086920	E-Mobility Charging Suite license codes for EV Charging Suite Setup	1.7.3 and earlier
1083065	IOL-CONF	1.7.0 and earlier

### **Impact**

An attacker may use the above-described vulnerabilities to perform a Denial of Service attack. Phoenix Contact devices using CodeMeter embedded are not affected by these vulnerabilities.

### **Classification of Vulnerability**

CVE-2021-20093:

Base Score: 9.1

Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:H

For details, please refer to WIBU Security Advisory [WIBU-210423-01](#)

CVE-2021-20094:

Base Score: 7.5

Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H

For details, please refer to WIBU Security Advisory [WIBU-210423-02](#)

### **Temporary Fix / Mitigation**

1. Use general security best practices to protect systems from local and network attacks like described in the application node [AH EN INDUSTRIAL SECURITY](#).
2. Run CodeMeter as client only and use localhost as binding for the CodeMeter communication. With binding to localhost an attack is no longer possible via remote network connection. The network server is disabled by default. If it is not possible to disable the network server, using a host-based firewall to restrict access to the CmLAN port can reduce the risk.
3. The CmWAN server is disabled by default. Please check if CmWAN is enabled and disable the feature if it is not needed.
4. Run the CmWAN server only behind a reverse proxy with user authentication to prevent attacks from unauthenticated users. The risk of an unauthenticated attacker can be further reduced by using a host-based firewall that only allows the reverse proxy to access the

CmWAN port.

### **Remediation**

PHOENIX CONTACT strongly recommends affected Users to upgrade to Codemeter V7.21a, which fixes these vulnerabilities. Wibu-Systems has already published this update for CodeMeter on their homepage. Since this current version of CodeMeter V7.21a has not yet been incorporated into Phoenix Contact products, we strongly recommend to download and install the current CodeMeter version directly from the [Wibu-Systems homepage](#).

### **Acknowledgement**

This vulnerability was discovered and reported to WIBU Systems by Tenable. We kindly appreciate the coordinated disclosure of this vulnerability by the finder.

PHOENIX CONTACT thanks CERT@VDE for the coordination and support with this publication.