

Phoenix Contact GmbH & Co. KG Flachsmarktstraße 8 32825 Blomberg, Germany Telefon: +49 5235 300

Internet: http://www.phoenixcontact.com

USt-Id-Nr.: DE124613250 WEEE-Reg.-Nr.: DE50738265

Telefax: +49 5235 3-41200

Phoenix Contact GmbH & Co. KG · 32825 Blomberg



Security Advisory for PHOENIX CONTACT products utilizing **WIBU-SYSTEMS CodeMeter Runtime.**

Publication Date: 2023-09-19 Last Update: 2023-11-11

Current Version: V1.2

Advisory Title

Denial of Service vulnerability in WIBU-SYSTEMS CodeMeter Runtime.

Advisory ID

CVE-2023-3935 VDE-2023-030

Vulnerability Description

A heap buffer overflow vulnerability in WIBU CodeMeter Runtime network service up to version 7.60b allows an unauthenticated remote attacker to achieve RCE and gain full access to the host system.



Affected products

Article no	Article	Affected versions
	Phoenix Contact Activation Wizard	<= 1.6
1046008	PLCnext Engineer	<= 2023.6
1165889	PLCNEXT ENGINEER EDU LIC	<= 2023.6
	(license codes)	
2702889	FL Network Manager	<= 7.0
1153509, 1153513, 1086929,	E-Mobility Charging Suite	<= 1.7.0
1153516, 1086891, 1153508,		
1153520, 1086921, 1086889,		
1086920		
1373907, 1373909, 1373233,	MORYX Software Platform	
1373910, 1373226, 1373236,	(CodeMeter is not directly integrated	
1373231, 1373224, 1373913,	and delivered together with MORYX	
1373912, 1373238, 1373914,	software.	
1373915, 1373916, 1373917,		
1373918, 1373908, 1550573,	CodeMeter is delivered with the linked	
1550576, 1550581, 1550587,	tool "Phoenix Contact Activation	
1550580, 1550582, 1532628,	Wizard". See line 1)	
1550574, 1550589		
1083065	IOL Conf	<= 1.7.0
1636198	MTP DESIGNER	<= 1.2.0 BETA
1636200	MTP DESIGNER TRIAL	

Impact

An attacker may use the above-described vulnerability to perform a remote code execution. Phoenix Contact devices using CodeMeter embedded are not affected by these vulnerabilities.

Classification of Vulnerability

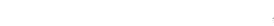
CVE-2023-3935 Base Score: 9.8

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

CWE-787: Out-of-bounds Write

CVE score and vector may have changed since publication of this advisory. You can find the current rating of a CVE at the respective link to the NVD website provided above.

...



Temporary Fix / Mitigation

- 1. Use general security best practices to protect systems from local and network attacks like described in the application node <u>AH EN INDUSTRIAL SECURITY</u>.
- 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 network for reducing the risk is strongly recommended.
- 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 V7.60c, which fixes this vulnerability. WIBU-SYSTEMS has already published this update for CodeMeter on their homepage. Since this current version of CodeMeter V7.60c 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.

Update Phoenix Contact Activation Wizard to version 1.7 when available. Please check the Phoenix Contact e-Shop for your related Software product regularly.

Acknowledgement

This vulnerability was discovered by WIBU-SYSTEMS.

We kindly appreciate the coordinated disclosure of this vulnerability.

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

History

V1.0 (2023-09-19): Initial publication

V1.1 (2023-10-11): Adjustment of the CVSS scores to reflect the changes made by NVD

V1.2 (2023-11-11): Removed CVE-2023-4701 because it was revoked.