Phoenix Contact Inc.
P.O. BOX 4100
Harrisburg, PA 17111-0100
Phone: 717-944-1300

Product Change Notification

PCN-AS-9110-2023

Business Unit	Product Line Code	Type of Change	Action	Date of Issue
AS - Automation Systems	DRD	Product Change Notification	Notify Distributors and Field	10/20/2023

The following Phoenix Contact products have been modified. Existing specifications will be met or exceeded. Please review and acknowledge this document and inform your personnel as needed.

Product Change Notification

Description for Product Change Notification

Advisory Title

Denial of Service vulnerabilities in WIBU-SYSTEMS CodeMeter Runtime.

Advisory ID

CVE-2023-3935
CVE-2023-4701
VDE-2023-030

Vulnerability Description

CVE-2023-3935: 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.

CVE-2023-4701: An Improper Privilege Management vulnerability through an incorrect use of privileged APIs in CodeMeter Runtime versions prior to 7.60c allow a local, low privileged attacker to use an API call for escalation of privileges in order gain full admin access on the host system

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: 10.0
Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H
CWE-787: Out-of-bounds Write

CVE-2023-4701
Base Score: 8.8
Vector: CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:C/C:H/I:H/A:H
CWE-269: Improper Privilege Management

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 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 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.

Product Change Notification

Remediation

PHOENIX CONTACT strongly recommends affected users to upgrade to CodeMeter V7.60c, which fixes these vulnerabilities. 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.

Note

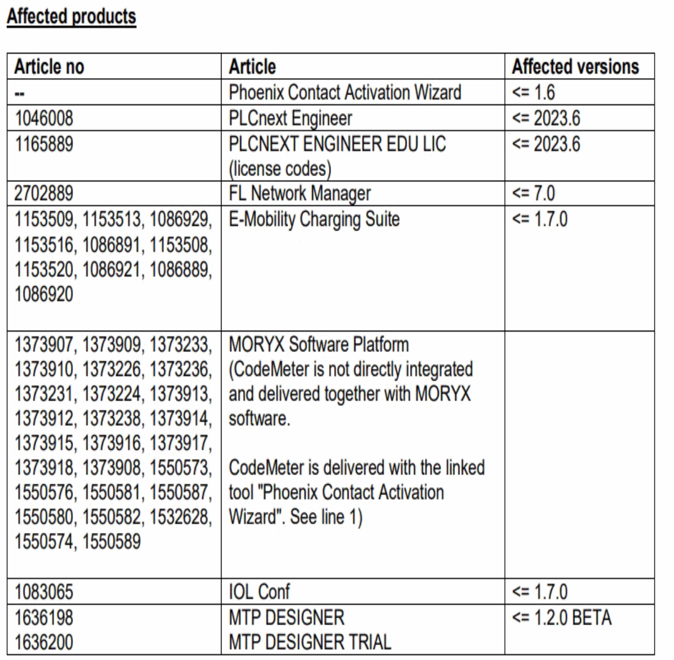
There are a number of software products not released in the US or that do not have a part number that are covered by this notice. Chief amongst this is the "Phoenix Contact Activation Wizard. Please check the attached picture for all of the products that are covered by this notice

Stock Status
Can existing stock still be used?
Is mixture of stock acceptable?

Transaction Dates	
Date modification goes into effect from Germany:	10/20/2023
Expected first shipment (from Phoenix Contact) of the modified products(s):	10/20/2023

Product Change Notification

Previous Product	New Product



Affected products

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

Should you have any issues with the timeline or content of this product change, please contact Phoenix Contact using the information below. Customers should acknowledge receipt of the PCN within 30 days of delivery of the PCN; provided, however, that the failure to acknowledge receipt does not affect the product change or the effective date thereof.

Contact Info:
Ted Thayer
tthayer@phoenixcontact.com

Thank you,

Zachary Stank

Product Marketing Manager

Product Change Notification

Part #	Type Description
	PLCNEXT ENGINEER
2702889	FL NETWORK MANAGER BASIC
1083065	IOL-CONF