Phoenix Contact GmbH & Co. KG
Flachsmarktstraße 8
32825 Blomberg, Germany
Telefon: +49 5235 300
Telefax: +49 5235 3-41200
Internet: http://www.phoenixcontact.com
USt-Id-Nr.: DE124613250
WEEE-Reg.-Nr.: DE50738265

Phoenix Contact GmbH & Co. KG · 32825 Blomberg

years of passion for technology and innovation

21 November 2023
2023/00015

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

| | |
|---|---|
| Publication Date: | 2023-11-21 |
| Last Update: | 2023-11-21 |
| Current Version: | V1.0 |

## Advisory Title

A Heap-based buffer overflow caused by libcurl, and wrong whitespace character interpretation in Javascript, both used in CodeMeter Runtime are affecting multiple products.

## Advisory ID

CVE-2023-38545
CVE-2023-24540
VDE-2023-062

## Vulnerability Description

**CVE-2023-38545:** The affected Wibu-Systems' products internally use the libcurl in a version that is vulnerable to a buffer overflow attack if curl is configured to redirect traffic through a SOCKS5 proxy. A malicious proxy can exploit a bug in the implemented handshake to cause a buffer overflow. If no SOCKS5 proxy has been configured, there is no attack surface.

Registered office: Blomberg
Distr. court Lemgo HRA 3746
Personally liable partner:
Phoenix Contact Verwaltungs-GmbH
Management office Blomberg
Distr. court Lemgo HRB 10904
Statutory seat Vaduz/Liechtenstein
Comm. reg. FL-0002.700.066-3

Group Executive Board:
Frank Stührenberg (CEO)
Dirk Görlitzer, Torsten Janwlecke
Ulrich Leidecker
Frank Possel-Dölken, Axel Wachholz
Chairman of the Advisory Board:
Dr. Dipl.-Ing. Eberhard Veit

Deutsche Bank AG
(BLZ 360 700 50) 226 2665 00
BIC: DEUTDEDEXXX
IBAN:
DE93 3607 0050 0226 2665 00

Commerzbank AG
(BLZ 476 400 51) 226 0396 00
BIC: COBADEFFXXX
IBAN:
DE31 4764 0051 0226 0396 00

...

**CVE-2023-24540:** Not all valid JavaScript whitespace characters are considered to be whitespace. Templates containing whitespace characters outside of the character set "\t\n\f\r\u0020\u2028\u2029" in JavaScript contexts that also contain actions may not be properly sanitized during execution.

## Affected products

| Article no | Article | Affected versions |
|---|---|---|
| -- | Phoenix Contact Activation Wizard | <= 1.6 |
| 1046008 | PLCnext Engineer | <= 2023.9 |
| 1165889 | PLCNEXT ENGINEER EDU LIC (license codes) | <= 2023.9 |
| 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.<br>CodeMeter is delivered with the linked tool "Phoenix Contact Activation Wizard". See line 1) | |
| 1083065 | IOL Conf | <= 1.7.0 |
| 1636198<br>1636200 | MTP DESIGNER<br>MTP DESIGNER TRIAL | <= 1.2.0 BETA |

## Impact

**CVE-2023-38545:** In a worst-case scenario and when using a SOCKS5 proxy, a successful exploitation of the vulnerability can lead to arbitrary code execution using the privileges of the user running the affected software.

**CVE-2023-24540:** WIBU Systems states that WIBU Codemeter is not affected by this vulnerability.

## Classification of Vulnerability

CVE-2023-38545
Base Score: 9.8
Vector: CVSS: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H
CWE: CWE-787

CVE-2023-24540
Base Score: 9.8
Vector: CVSS: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H
CWE: CWE-74

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

Disable using a SOCKS5 proxy:

- The proxy environment variables HTTP_PROXY, HTTPS_PROXY and ALL_PROXY must not be set to socks5h://
- Ensure that CodeMeter is not defined to use the SOCKS5 proxy. The variable ProxyServer must not be start with socks5h://.
    - On Windows, the definition of that variable is in the registry (regedit) under HKLM/SOFTWARE/WIBU-SYSTEMS/CodeMeter/Server/CurrentVersion
    - On Mac, the definition of that variable is in the file /Library/Preferences/com.wibu.CodeMeter.Server.ini
    - On Linux, the definition of that variable is in the file /etc/wibu/CodeMeter/Server.ini
    - On Solaris, the definition of that variable is in the file /etc/opt/CodeMeter/Server.ini

Use general security best practices to protect systems from local and network attacks like described in the application node AH EN INDUSTRIAL SECURITY.

...

## Remediation

PHOENIX CONTACT strongly recommends affected users to upgrade to CodeMeter V7.60d, which fixes these vulnerabilities. WIBU-SYSTEMS has already published an update for CodeMeter on their homepage. Since this current version of CodeMeter V7.60d 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 related Software updates regularly.

## Acknowledgement

Phoenix Contact was informed about these vulnerabilities by WIBU-SYSTEMS.
We kindly appreciate the coordinated disclosure of these vulnerabilities by the finder.

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

## History

V1.0 (2023-11-21): Initial publication