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

08 September 2020
300488800/pbsa56

Security Advisory for PHOENIX CONTACT products utilizing WIBU SYSTEMS CodeMeter components

Advisory Title

Several vulnerabilities have been discovered in WIBU SYSTEMS CodeMeter Runtime.

Advisory ID

CVE-2020-14509, CVE-2020-14519, CVE-2020-16233
VDE-2020-030

Vulnerability Description

Several vulnerabilities have been discovered in WIBU SYSTEMS CodeMeter and published 08 September 2020. Phoenix Contact is only affected by a subset of these vulnerabilities.

WIBU Security Advisory	CVE Number	Description	CVSS v3.1 Base Score
WIBU-200521-02	CVE-2020-14519	CodeMeter Runtime WebSockets API: Missing Origin Validation	High 8.1 AV:N/AC:L/PR:N/UI:R/S:U/C:N/I:H/A:H
WIBU-200521-03	CVE-2020-14509	CodeMeter Runtime DoS due to Buffer Access with Incorrect Length Value	Critical 10.0 AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H
WIBU-200521-05	CVE-2020-16233	CodeMeter Runtime API: Heap Leak	High 7.5 AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N

Phoenix Contact products are not affected by vulnerabilities WIBU-200521-01 (CVE-2020-14513), WIBU-200521-04 (CVE-2020-14517, and WIBU-200521-06 (CVE-2020-14515).
For further Information please refer to WIBU Advisories directly at https://wibu.com/support/security-advisories.html.

Affected products

Article no	Article	Affected versions
1046008	PC Worx Engineer	2020.06 and earlier
1165889	PLCNEXT ENGINEER EDU LIC (License codes)	2020.06 and earlier
2702889	FL Network Manager	4.20 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

Impact

WIBU Security Advisory	CVE Number	Description	Phoenix Contact products according table above
WIBU-200521-01	CVE-2020-14513 Score: 7.5	Improper Input Validation of WibuRaU files in CodeMeter Runtime	Products **are not affected** as Phoenix Contact is using a Universal Firm Code
WIBU-200521-02	CVE-2020-14519 Score: 8.1	CodeMeter Runtime WebSockets API: Missing Origin Validation	Products are affected according WIBU Systems classification
WIBU-200521-03	CVE-2020-14509 Score: 10.0	CodeMeter Runtime DoS due to Buffer Access with Incorrect Length Value	Products are affected according WIBU Systems classification
WIBU-200521-04	CVE-2020-14517 Score: 9.4	CodeMeter Runtime API: Inadequate Encryption Strength and Authentication	Products **are not affected** as Phoenix Contact is using AxProtector
WIBU-200521-05	CVE-2020-16233 Score: 7.5	CodeMeter Runtime API: Heap Leak	Products are affected according WIBU Systems classification
WIBU-200521-06	CVE-2020-14515 Score: 7.4	Improper Signature Verification of CmActLicense update files for CmActLicense Firm Code	Products **are not affected** as Phoenix Contact is using a Universal Firm Code

Phoenix Contact devices using CodeMeter embedded are not affected by these vulnerabilities. According to WIBU SYSTEMS Universal Firm Codes (UFC) used by Phoenix Contact are not affected.

...

Classification of Vulnerability

For detailed information please refer to WIBU SYSTEMS original Advisories at https://wibu.com/support/security-advisories.html.

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. Disable the CodeMeter Runtime WebSockets API.
3. Run CodeMeter only as client and use localhost as binding for the CodeMeter communication. If you need to operate CodeMeter Runtime as Network License Server please make sure that it is operated in a secure environment.

For detailed information please refer to WIBU Systems original Advisories.

Remediation

WIBU SYSTEMS has released a new CodeMeter Runtime version 7.10 to fix the known vulnerabilities and may continue to release further updated versions in the future.

Phoenix Contact has released a new version of Activation Wizard 1.3.2, used for activation and deactivation of licenses, installing CodeMeter Runtime 7.10 on Windows PCs.
After installation of Activation Wizard 1.3.2 all installed products using CodeMeter Runtime will use the latest CodeMeter Runtime 7.10 version.
Activation Wizard 1.3.2 contains the official fix of WIBU SYSTEMS for the known variabilities and is disabling the WebSockets API like recommended by WIBU SYSTEMS.

We strongly recommend downloading and installing Activation Wizard 1.3.2 or higher as the CVSS Score of the vulnerabilities are critical and high. Activation Wizard is available via the download areas of PLCnext Engineer,. FL Network Manager, or EV Charging Suite.
Since there can only be one installation of CodeMeter Runtime on a system, installing the latest version of CodeMeter Runtime as being included in Activation Wizard will fix the vulnerabilities for all other applications using CodeMeter Runtime as well.

Please check your products web site for further updates regularly or register to Phoenix Contact PSIRT information’s to receive latest updates about security advisories.

Phoenix Contact recommends following security best practices to protect systems form local and network attacks as described in the application note AH EN INDUSTRIAL SECURITY.

Acknowledgement

This Advisory is published in Coordinated Disclosure with WIBU SYSTEMS and the original finders and CERTs involved.