TLP:WHITE

VDE-2025-064: Phoenix Contact: Products utilizing WIBU-SYSTEMS CodeMeter Runtime Windows Installer have a privilege escalation

Publisher: Phoenix Contact GmbH & Co. KG	Document category: csaf_security_advisory
Initial release date: Tue Sep 09 09:00:00 CEST 2025	Engine: 2.5.33
Current release date: Tue Sep 09 09:00:00 CEST 2025	Build Date: Mon Aug 25 10:47:01 CEST 2025
Current version: 1	Status: FINAL
CVSSv3.1 Base Score: 8.2	Severity: High
Original language: en	Language: en-GB
Also referred to: VDE-2025-064, PCSA-2025-00011	

Summary

A local privilege escalation vulnerability in Phoenix Contact products utilizing WIBU-SYSTEMS CodeMeter Runtime allows users to gain admin rights on freshly installed systems. The CodeMeter Control Center starts with elevated privileges and retains them until restarted, enabling unauthorized access to admin tools like cmd.exe.

General Recommendation

Phoenix Contact recommends operating network-capable devices in closed networks or protected with a suitable firewall. For detailed information on our recommendations for measures to protect network-capable devices, please refer to our application note.

Impact

The effect is that CodeMeter Control Center can be launched once as administrator and will remain with these privileges until it is either manually closed or the user is logged out. In this case a malicious user can navigate, for example, to C:\Windows\System32\ and right-click on cmd.exe and select "open", thus getting an administrator console. This vulnerability only affects freshly installed systems until CodeMeter Control Center is restarted.

Remediation

PHOENIX CONTACT strongly recommends affected users to upgrade to CodeMeter V8.30a, which fixes these vulnerabilities. WIBU-SYSTEMS has already published this update for CodeMeter on their homepage. Since this current version of CodeMeter V8.30a 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.

Additional Recommendations: Regularly check the product's official webpage for updated release versions that support CodeMeter V8.30a. Update the Activation Wizard to version 1.8 as soon as it becomes available on the product's download page.

Mitigation

After installing the CodeMeter Control Center (at least once), please perform one of the following actions:

- Restart your system
- Log-out and log-in in
- Manually close or restart the CodeMeter Control Center via the system tray icon

These steps must be followed immediately after installing the CodeMeter Runtime or any product that includes the CodeMeter Runtime.

Product groups

Affected Products.

- Activation Wizard <1.8
- PLCnext Engineer <2025.0.3
- PLCnext Engineer EDU LIC <2025.0.3
- FL Network Manager <=8.0
- EV Charging Suite (all versions) <=1.7.0
- EV Charging Suite (all upgrades) <=1.7.0
- CLIPX ENGINEER ASSEMBLE <=1.0.0
- MLnext Execution <=1.1.3
- MTP DESIGNER / MTP DESIGNER TRAIL <=1.3.1
- Activation Wizard <1.8 installed with MORYX-Software Platform
- MLnext Creation <=24.10.0

Fixed Products.

- PLCnext Engineer 2025.0.3
- PLCnext Engineer EDU LIC 2025.0.3
- Activation Wizard 1.8

Vulnerabilities

CVE-2025-47809

Vulnerability Description

Wibu CodeMeter before 8.30a sometimes allows privilege escalation immediately after installation (before a logoff or reboot). For exploitation, there must have been an unprivileged installation with UAC, and the CodeMeter Control Center component must be installed, and the CodeMeter Control Center component must not have been restarted. In this scenario, the local user can navigate from Import License to a privileged instance of Windows Explorer.

CWE: CWE-272: Least Privilege Violation

Product status

Known affected

Product	CVSS-Vector	CVSS Base Score
Activation Wizard <1.8	CVSS:3.1/AV:L/AC:L/PR:L/UI:R/S:C/C:H/I:H/A:H	8.2
PLCnext Engineer <2025.0.3 Order number: 1046008	CVSS:3.1/AV:L/AC:L/PR:L/UI:R/S:C/C:H/I:H/A:H	8.2
PLCnext Engineer EDU LIC <2025.0.3 Order number: 1165889	CVSS:3.1/AV:L/AC:L/PR:L/UI:R/S:C/C:H/I:H/A:H	8.2
FL Network Manager <=8.0 Order number: 2702889	CVSS:3.1/AV:L/AC:L/PR:L/UI:R/S:C/C:H/I:H/A:H	8.2
EV Charging Suite (all versions) <=1.7.0 Order number: 1153509 Order number: 1153508 Order number: 1128335 Order number: 1086929 Order number: 1086921 Order number: 1086920	CVSS:3.1/AV:L/AC:L/PR:L/UI:R/S:C/C:H/I:H/A:H	8.2
EV Charging Suite (all upgrades) <=1.7.0 Order number: 1153520 Order number: 1153516 Order number: 1153513 Order number: 1086891 Order number: 1086889	CVSS:3.1/AV:L/AC:L/PR:L/UI:R/S:C/C:H/I:H/A:H	8.2
CLIPX ENGINEER ASSEMBLE <=1.0.0 Order number: 1662166	CVSS:3.1/AV:L/AC:L/PR:L/UI:R/S:C/C:H/I:H/A:H	8.2
MLnext Execution <=1.1.3 Order number: 1391115	CVSS:3.1/AV:L/AC:L/PR:L/UI:R/S:C/C:H/I:H/A:H	8.2
MORYX-Software Platform Order number: 1373907 Order number: 1373909 Order number: 1373233 Order number: 1373910 Order number: 1373226 Order number: 1373236 Order number: 1373231 Order number: 1373224 Order number: 1373913 Order number: 1373912 Order number: 1373238 Order number: 1373914 Order number: 1373915 Order number: 1373916 Order number: 1373917 Order number: 1373918 Order number: 1373908 Order number: 1550573 Order number: 1550576 Order number: 1550581 Order number: 1550587 Order number: 1550580 Order number: 1550582 Order number: 1532628 Order number: 1550574 Order number: 1550589	CVSS:3.1/AV:L/AC:L/PR:L/UI:R/S:C/C:H/I:H/A:H	8.2
MLnext Creation <=24.10.0 Order number: 1697763	CVSS:3.1/AV:L/AC:L/PR:L/UI:R/S:C/C:H/I:H/A:H	8.2

Fixed

Product
PLCnext Engineer 2025.0.3 Order number: 1046008 (Download)
PLCnext Engineer EDU LIC 2025.0.3 Order number: 1165889 (Download)
Activation Wizard 1.8

Acknowledgments

Phoenix Contact GmbH & Co. KG thanks the following parties for their efforts:

- CERT@VDE for coordination. (see: https://certvde.com)
- WIBU-SYSTEMS for reporting.

Phoenix Contact GmbH & Co. KG

Namespace: https://phoenixcontact.com/psirt

psirt@phoenixcontact.com

References

- PCSA-2025-00011 (EXTERNAL): https://phoenixcontact.com/psirt
- Phoenix Contact advisory overview at CERT@VDE (EXTERNAL): https://certvde.com/de/advisories/vendor/phoenixcontact/
- Phoenix Contact application note (EXTERNAL): https://dam-mdc.phoenixcontact.com/asset/156443151564/0a870ae433c19148b80bd760f3a1c1f2/107913_en_03.pdf
- VDE-2025-064: Phoenix Contact: Products utilizing WIBU-SYSTEMS CodeMeter Runtime Windows Installer have a privilege escalation - HTML (SELF): https://certvde.com/en/advisories/VDE-2025-064
- VDE-2025-064: Phoenix Contact: Products utilizing WIBU-SYSTEMS CodeMeter Runtime Windows Installer have a privilege escalation - CSAF (SELF): https://phoenixcontact.csaf-tp.certvde.com/.well-known/csaf/white/2025/vde-2025-064.json

Revision history

Version	Date of the revision	Summary of the revision
1	Tue Sep 09 09:00:00 CEST 2025	Initial

Sharing rules

TLP:WHITE

For the TLP version see https://www.first.org/tlp/