VDE-2026-084: Phoenix Contact: CodeMeter Runtime Security Vulnerabilities in License Validation in the PLCnext Firmware

Publisher: Phoenix Contact GmbH & Co. KG	Document category: csaf_security_advisory
Initial release date: Wed Nov 04 10:00:00 CET 2026	Engine: 2.6.12
Current release date: Wed Nov 04 10:00:00 CET 2026	Build Date: Thu Oct 15 10:22:03 CEST 2026
Current version: 1.0.0	Status: FINAL
CVSSv3.1 Base Score: 8.6	Severity: High
Original language: en	Language: en-GB
Also referred to: VDE-2026-084, PCSA-2026-00009	

Summary

This advisory addresses security vulnerabilities in Phoenix Contact products with an integrated CodeMeter Runtime, like PLCnext devices and Virtual Controls. These security vulnerabilities only may occur with versions <8.41a of the integrated software CodeMeter Runtime from Wibu-Systems. Please see listed products to determine which devices and firmware versions are affected.

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 reported vulnerabilities allow unauthenticated attackers to read and overwrite sensitive configuration data and to crash CodeMeter Runtime which has only an impact on the licensing infrastructure. Licenses then are not accessible anymore. These security vulnerabilities may occur on PLCnext devices or Virtual Controls with an integrated CodeMeter Runtime (see affected products).

Remediation

Please check the Phoenix Contact e-Shop regularly to see if the fixed firmware is already available for your specific PLCnext device or Virtual PLCnext Control. The Fix is planned to be integrated in version 2026.0.6 which is planned for Q4/2026.

© Phoenix Contact GmbH & Co. KG
Flachsmarktstraße 8, D-32825 Blomberg, Germany

Mitigation

For affected PLCnext devices and Virtual Controls with an integrated Codemeter Runtime (see affected products), PHOENIX CONTACT strongly recommends to follow the descriptions below:

On PLCnext devices switch on the firewall via the WBM to avoid an unauthenticated access.

Affected Product(s)

Article	Name	Affected	Fixed
1151412	AXC F 1152	Firmware 2025.0 <2026.0.6 installed on AXC F 1152	Firmware 2026.0.6 installed on AXC F 1152
1646469	AXC F 1252	Firmware 2025.0 <2026.0.6 installed on AXC F 1252	Firmware 2026.0.6 installed on AXC F 1252
1551772	AXC F 2000 EA	Firmware 2025.0 <2026.0.6 installed on AXC F 2000 EA	Firmware 2026.0.6 installed on AXC F 2000 EA
2404267	AXC F 2152	Firmware 2025.0 <2026.0.6 installed on AXC F 2152	Firmware 2026.0.6 installed on AXC F 2152
1069208	AXC F 3152	Firmware 2025.0 <2026.0.6 installed on AXC F 3152	Firmware 2026.0.6 installed on AXC F 3152
1246285	BPC 9102S	Firmware 2025.0 <2026.0.6 installed on BPC 9102S	Firmware 2026.0.6 installed on BPC 9102S
1839159	BPC 9202S	Firmware 2025.0 <2026.0.6 installed on BPC 9202S	Firmware 2026.0.6 installed on BPC 9202S
1136419	RFC 4072R	Firmware 2025.0 <2026.0.6 installed on RFC 4072R	Firmware 2026.0.6 installed on RFC 4072R
1051328	RFC 4072S	Firmware 2025.0 <2026.0.6 installed on RFC 4072S	Firmware 2026.0.6 installed on RFC 4072S
1760157	VL3 UPC 2440 EDGE	Firmware 2025.0 <2026.0.6 installed on VL3 UPC 2440 EDGE	Firmware 2026.0.6 installed on VL3 UPC 2440 EDGE
1737875	VPLCNEXT CONTROL 1000	Firmware 2025.0 <2026.0.6 installed on VPLCNEXT CONTROL 1000	Firmware 2026.0.6 installed on VPLCNEXT CONTROL 1000
1738453	VPLCNEXT CONTROL 2000	Firmware 2025.0 <2026.0.6 installed on VPLCNEXT CONTROL 2000	Firmware 2026.0.6 installed on VPLCNEXT CONTROL 2000
1738454	VPLCNEXT CONTROL 3000	Firmware 2025.0 <2026.0.6 installed on VPLCNEXT CONTROL 3000	Firmware 2026.0.6 installed on VPLCNEXT CONTROL 3000
1751491	VPLCNEXT CONTROL 500	Firmware 2025.0 <2026.0.6 installed on VPLCNEXT CONTROL 500	Firmware 2026.0.6 installed on VPLCNEXT CONTROL 500
1886438	Catan C1	CodeMeter Runtime 8.0 <8.41a Firmware 2026.0 <2026.0.6 installed on Catan C1	CodeMeter Runtime 8.41a Firmware 2026.0.6 installed on Catan C1

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. (see: https://www.wibu.com/support/security-advisories.html)

© Phoenix Contact GmbH & Co. KG
Flachsmarktstraße 8, D-32825 Blomberg, Germany

- Vector Informatik GmbH Andrew Teylu for Reporting.

Phoenix Contact GmbH & Co. KG

Namespace: https://phoenixcontact.com/psirt

psirt@phoenixcontact.com

References

- PCSA-2026-00009 (EXTERNAL): https://phoenixcontact.com/psirt
- Phoenix Contact advisory overview at CERT@VDE (EXTERNAL): https://certvde.com/de/advisories/vendor/phoenixcontact
- VDE-2026-084: Phoenix Contact: CodeMeter Runtime Security Vulnerabilities in License Validation in the PLCnext Firmware - HTML (SELF): https://certvde.com/en/advisories/vde-2026-084
- VDE-2026-084: Phoenix Contact: CodeMeter Runtime Security Vulnerabilities in License Validation in the PLCnext Firmware - CSAF (SELF): https://phoenixcontact.csaf-tp.certvde.com/.well-known/csaf/white/2026/vde-2026-084.json

Revision history

Version	Date of the revision	Summary of the revision
1.0.0	Wed Nov 04 10:00:00 CET 2026	Initial

Sharing rules

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

© Phoenix Contact GmbH & Co. KG
Flachsmarktstraße 8, D-32825 Blomberg, Germany

Vulnerability Details

Improper Access Control in Local-Only Configuration Commands (CVE-2026-81573)

CVE Description

If CodeMeter Runtime is configured as a server, the configuration command handler does not enforce network-origin restrictions. Commands intended only for local or same-network clients can therefore be executed by arbitrary remote peers. An attacker can read potentially sensitive configuration data and overwrite selected values in Server.ini. This does include the hash of the credentials for the CodeMeter WebAdmin, enabling WebAdmin takeover.

CWE:	CWE-284: Improper Access Control

Product status

Known affected

Product	CVSS-Vector	CVSS Base Score
AXC F 1152 Firmware 2025.0 <2026.0.6 installed on AXC F 1152 Order number: 1151412	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:C/C:N/I:N/A:H	8.6
AXC F 1252 Firmware 2025.0 <2026.0.6 installed on AXC F 1252 Order number: 1646469	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:C/C:N/I:N/A:H	8.6
AXC F 2152 Firmware 2025.0 <2026.0.6 installed on AXC F 2152 Order number: 2404267	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:C/C:N/I:N/A:H	8.6
AXC F 3152 Firmware 2025.0 <2026.0.6 installed on AXC F 3152 Order number: 1069208	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:C/C:N/I:N/A:H	8.6
BPC 9102S Firmware 2025.0 <2026.0.6 installed on BPC 9102S Order number: 1246285	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:C/C:N/I:N/A:H	8.6
BPC 9202S Firmware 2025.0 <2026.0.6 installed on BPC 9202S Order number: 1246285	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:C/C:N/I:N/A:H	8.6
RFC 4072R Firmware 2025.0 <2026.0.6 installed on RFC 4072R Order number: 1136419	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:C/C:N/I:N/A:H	8.6
RFC 4072S Firmware 2025.0 <2026.0.6 installed on RFC 4072S Order number: 1051328	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:C/C:N/I:N/A:H	8.6
VL3 UPC 2440 EDGE Firmware 2025.0 <2026.0.6 installed on VL3 UPC 2440 EDGE Order number: 1760157	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:C/C:N/I:N/A:H	8.6
VPLCNEXT CONTROL 1000 Firmware 2025.0 <2026.0.6 installed on VPLCNEXT CONTROL 1000 Order number: 1737875	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:C/C:N/I:N/A:H	8.6

© Phoenix Contact GmbH & Co. KG
Flachsmarktstraße 8, D-32825 Blomberg, Germany

Product	CVSS-Vector	CVSS Base Score
VPLCNEXT CONTROL 2000 Firmware 2025.0 <2026.0.6 installed on VPLCNEXT CONTROL 2000 Order number: 1738453	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:C/C:N/I:N/A:H	8.6
VPLCNEXT CONTROL 3000 Firmware 2025.0 <2026.0.6 installed on VPLCNEXT CONTROL 3000 Order number: 1738454	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:C/C:N/I:N/A:H	8.6
VPLCNEXT CONTROL 500 Firmware 2025.0 <2026.0.6 installed on VPLCNEXT CONTROL 500 Order number: 1751491	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:C/C:N/I:N/A:H	8.6
Catan C1 Firmware 2026.0 <2026.0.6 installed on Catan C1 Order number: 1886438	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:C/C:N/I:N/A:H	8.6
Catan C1 CodeMeter Runtime 8.0 <8.41a	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:C/C:N/I:N/A:H	8.6

Format String Vulnerability in Logger (CVE-2026-81574)

CVE Description

The logger does not sanitize input strings in certain cases, allowing an attacker to inject printf-style format specifiers. This can be used to reliably crash CodeMeter and disclose sensitive information such as process memory and stack canaries. The attack works locally, for example by using cmu --set-proxy to set the proxy value, and remotely when combined with CVE-2026-81573 by setting General.ProxyServer and then triggering this vulnerability.

CWE:	CWE-134: Use of Externally-Controlled Format String

Product status

Known affected

Product	CVSS-Vector	CVSS Base Score
AXC F 1152 Firmware 2025.0 <2026.0.6 installed on AXC F 1152 Order number: 1151412	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:H	8.2
AXC F 1252 Firmware 2025.0 <2026.0.6 installed on AXC F 1252 Order number: 1646469	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:H	8.2
AXC F 2000 EA Firmware 2025.0 <2026.0.6 installed on AXC F 2000 EA Order number: 1551772	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:H	8.2
AXC F 2152 Firmware 2025.0 <2026.0.6 installed on AXC F 2152 Order number: 2404267	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:H	8.2
AXC F 3152 Firmware 2025.0 <2026.0.6 installed on AXC F 3152 Order number: 1069208	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:H	8.2
BPC 9102S Firmware 2025.0 <2026.0.6 installed on BPC 9102S	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:	8.2

© Phoenix Contact GmbH & Co. KG
Flachsmarktstraße 8, D-32825 Blomberg, Germany

Product	CVSS-Vector	CVSS Base Score
Order number: 1246285	L/I:N/A:H	
BPC 9202S Firmware 2025.0 <2026.0.6 installed on BPC 9202S Order number: 1246285	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:H	8.2
RFC 4072R Firmware 2025.0 <2026.0.6 installed on RFC 4072R Order number: 1136419	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:H	8.2
RFC 4072S Firmware 2025.0 <2026.0.6 installed on RFC 4072S Order number: 1051328	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:H	8.2
VL3 UPC 2440 EDGE Firmware 2025.0 <2026.0.6 installed on VL3 UPC 2440 EDGE Order number: 1760157	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:H	8.2
VPLCNEXT CONTROL 1000 Firmware 2025.0 <2026.0.6 installed on VPLCNEXT CONTROL 1000 Order number: 1737875	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:H	8.2
VPLCNEXT CONTROL 2000 Firmware 2025.0 <2026.0.6 installed on VPLCNEXT CONTROL 2000 Order number: 1738453	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:H	8.2
VPLCNEXT CONTROL 3000 Firmware 2025.0 <2026.0.6 installed on VPLCNEXT CONTROL 3000 Order number: 1738454	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:H	8.2
VPLCNEXT CONTROL 500 Firmware 2025.0 <2026.0.6 installed on VPLCNEXT CONTROL 500 Order number: 1751491	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:H	8.2
Catan C1 Firmware 2026.0 <2026.0.6 installed on Catan C1 Order number: 1886438	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:H	8.2
Catan C1 CodeMeter Runtime 8.0 <8.41a	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:H	8.2

Missing Sanity Checks for Buffer Lengths (CVE-2026-81575)

CVE Description

If configured as a server, CodeMeter Runtime accepts requests with opcode 0x5e, which contain the data length and the data itself. Missing bounds checking on the data length value can lead to out of bounds reads, causing a segmentation fault that ultimately crashes the CodeMeter Runtime.

CWE:	CWE-130: Improper Handling of Length Parameter Inconsistency

Product status

© Phoenix Contact GmbH & Co. KG
Flachsmarktstraße 8, D-32825 Blomberg, Germany

Known affected

Product	CVSS-Vector	CVSS Base Score
AXC F 1152 Firmware 2025.0 <2026.0.6 installed on AXC F 1152 Order number: 1151412	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H	7.5
AXC F 1252 Firmware 2025.0 <2026.0.6 installed on AXC F 1252 Order number: 1646469	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H	7.5
AXC F 2000 EA Firmware 2025.0 <2026.0.6 installed on AXC F 2000 EA Order number: 1551772	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H	7.5
AXC F 2152 Firmware 2025.0 <2026.0.6 installed on AXC F 2152 Order number: 2404267	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H	7.5
AXC F 3152 Firmware 2025.0 <2026.0.6 installed on AXC F 3152 Order number: 1069208	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H	7.5
BPC 9102S Firmware 2025.0 <2026.0.6 installed on BPC 9102S Order number: 1246285	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H	7.5
BPC 9202S Firmware 2025.0 <2026.0.6 installed on BPC 9202S Order number: 1246285	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H	7.5
RFC 4072R Firmware 2025.0 <2026.0.6 installed on RFC 4072R Order number: 1136419	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H	7.5
RFC 4072S Firmware 2025.0 <2026.0.6 installed on RFC 4072S Order number: 1051328	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H	7.5
VL3 UPC 2440 EDGE Firmware 2025.0 <2026.0.6 installed on VL3 UPC 2440 EDGE Order number: 1760157	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H	7.5
VPLCNEXT CONTROL 1000 Firmware 2025.0 <2026.0.6 installed on VPLCNEXT CONTROL 1000 Order number: 1737875	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H	7.5
VPLCNEXT CONTROL 2000 Firmware 2025.0 <2026.0.6 installed on VPLCNEXT CONTROL 2000 Order number: 1738453	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H	7.5
VPLCNEXT CONTROL 3000 Firmware 2025.0 <2026.0.6 installed on VPLCNEXT CONTROL 3000 Order number: 1738454	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H	7.5
VPLCNEXT CONTROL 500 Firmware 2025.0 <2026.0.6 installed on VPLCNEXT CONTROL 500 Order number: 1751491	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H	7.5
Catan C1 Firmware 2026.0 <2026.0.6 installed on Catan C1 Order number: 1886438	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H	7.5
Catan C1 CodeMeter Runtime 8.0 <8.41a	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H	7.5

Improper Authentication of Session Handles (CVE-2026-81576)

CVE Description

© Phoenix Contact GmbH & Co. KG
Flachsmarktstraße 8, D-32825 Blomberg, Germany

If configured as a server, CodeMeter Runtime issues handle per connection and relies on a cryptographically weak SID as sole authenticator. An attacker can brute-force the SID, recover another session's handle number, and read license information belonging to another handle.

CWE:	CWE-639: Authorization Bypass Through User-Controlled Key

Product status

Known affected

Product	CVSS-Vector	CVSS Base Score
AXC F 1152 Firmware 2025.0 <2026.0.6 installed on AXC F 1152 Order number: 1151412	CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:C/C:H/I:N/A:N	7.7
AXC F 1252 Firmware 2025.0 <2026.0.6 installed on AXC F 1252 Order number: 1646469	CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:C/C:H/I:N/A:N	7.7
AXC F 2000 EA Firmware 2025.0 <2026.0.6 installed on AXC F 2000 EA Order number: 1551772	CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:C/C:H/I:N/A:N	7.7
AXC F 2152 Firmware 2025.0 <2026.0.6 installed on AXC F 2152 Order number: 2404267	CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:C/C:H/I:N/A:N	7.7
AXC F 3152 Firmware 2025.0 <2026.0.6 installed on AXC F 3152 Order number: 1069208	CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:C/C:H/I:N/A:N	7.7
BPC 9102S Firmware 2025.0 <2026.0.6 installed on BPC 9102S Order number: 1246285	CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:C/C:H/I:N/A:N	7.7
BPC 9202S Firmware 2025.0 <2026.0.6 installed on BPC 9202S Order number: 1246285	CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:C/C:H/I:N/A:N	7.7
RFC 4072R Firmware 2025.0 <2026.0.6 installed on RFC 4072R Order number: 1136419	CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:C/C:H/I:N/A:N	7.7
RFC 4072S Firmware 2025.0 <2026.0.6 installed on RFC 4072S Order number: 1051328	CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:C/C:H/I:N/A:N	7.7
VL3 UPC 2440 EDGE Firmware 2025.0 <2026.0.6 installed on VL3 UPC 2440 EDGE Order number: 1760157	CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:C/C:H/I:N/A:N	7.7
VPLCNEXT CONTROL 1000 Firmware 2025.0 <2026.0.6 installed on VPLCNEXT CONTROL 1000 Order number: 1737875	CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:C/C:H/I:N/A:N	7.7
VPLCNEXT CONTROL 2000 Firmware 2025.0 <2026.0.6 installed on VPLCNEXT CONTROL 2000 Order number: 1738453	CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:C/C:H/I:N/A:N	7.7
VPLCNEXT CONTROL 3000 Firmware 2025.0 <2026.0.6 installed on VPLCNEXT CONTROL 3000 Order number: 1738454	CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:C/C:H/I:N/A:N	7.7
VPLCNEXT CONTROL 500 Firmware 2025.0 <2026.0.6 installed on VPLCNEXT CONTROL 500 Order number: 1751491	CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:C/C:H/I:N/A:N	7.7

© Phoenix Contact GmbH & Co. KG
Flachsmarktstraße 8, D-32825 Blomberg, Germany

Product	CVSS-Vector	CVSS Base Score
Catan C1 Firmware 2026.0 <2026.0.6 installed on Catan C1 Order number: 1886438	CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:C/C:H/I:N/A:N	7.7
Catan C1 CodeMeter Runtime 8.0 <8.41a	CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:C/C:H/I:N/A:N	7.7

© Phoenix Contact GmbH & Co. KG
Flachsmarktstraße 8, D-32825 Blomberg, Germany