VDE-2026-098: Phoenix Contact: CodeMeter Runtime Security Vulnerabilities in License Validation for SW Tools

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: Fri Sep 18 11:00:26 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-2026-098, PCSA-2026-00013	

Summary

This advisory addresses multiple security vulnerabilities in Phoenix Contact products using the software CodeMeter Runtime like licensed desktop software tools. These security vulnerabilities only may occur with CodeMeter Runtime 8.x versions <V8.41a and CodeMeter Runtime 9.x versions <9.10 from Wibu-Systems.

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 delete arbitrary files, to read and overwrite sensitive configuration data and to crash Codemeter Runtime. These security vulnerabilities may occur on systems with operating systems Windows, Linux and Mac with installed Phoenix Contact software tools (see affected products).

Remediation

Updates for the affected products are planned for Q4 2026. Until the fix is available, please follow the mitigation measures and check the respective product page on the Phoenix Contact website regularly to see if the fix is already available.

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

Product Name	Planned Fixed Version
Activation Wizard	1.8.2
PLCnext Engineer	2026.0.5 LTS
PLCnext Engineer EDU LIC	2026.0.5 LTS
FL Network Manager	10.0
CLIPX ENGINEER ASSEMBLE	1.3.1
MLnext Execution	2026.12
MLnext Creation	2026.12
IO-Link ENGINEER	6.0.1.11090
MARKING system	1.3

Mitigation

Phoenix Contact strongly recommends affected users to upgrade to CodeMeter Runtime >=V8.41a or >=V9.10, which fixes these vulnerabilities. WIBU-SYSTEMS has already published CodeMeter Runtime updates on their homepage. Since the updated versions of Codemeter Runtime have not yet been incorporated into Phoenix Contact software tools, we strongly recommend to download and install the updated CodeMeter Runtime version e.g. for Windows directly from the WIBU-SYSTEMS homepage.

If you enabled the network server functionality on a Windows, Linux or Mac-system at some point but no longer need it, disable it.

If you are using CodeMeter Runtime 9.00 or newer, you can use cmu --disable-network-server.

If you are using older versions of CodeMeter Runtime, do the following:

On Windows:

- Open the Registry Editor.
- Navigate to "computer\HKEY_LOCAL_MACHINE\SOFTWARE\WIBU-SYSTEMS\CodeMeter\Server\CurrentVersion".
- Then change the value of NetworkServer from 1 to 0.
- Restart CodeMeter.

On Linux and Mac:

- Stop CodeMeter.
- Edit the file under "/etc/wibu/CodeMeter/Server.ini": Under [General], change the value IsNetworkServer from 1 to 0. • Then start CodeMeter again.

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

Affected Product(s)

Article	Name	Affected	Fixed
	Activation Wizard	< 1.8.2	1.8.2
1046008	PLCnext Engineer	< 2026.0.5 LTS	2026.0.5
1165891	PLCnext Engineer EDU LIC	< 2026.0.5 LTS	2026.0.5
2702889	FL Network Manager	0.0 - 10.0	10.0
1662166	CLIPX ENGINEER ASSEMBLE	< 1.3.1	1.3.1
1391115	MLnext Execution	< 2026.12	2026.12
1697763	MLnext Creation	< 2026.12	2026.12
1534453	IO-Link ENGINEER	< 6.0.1.11090	6.0.1.11090
1669297	MARKING system	< 1.3	1.3
1636198	MTP DESIGNER	< 1.3.3	
1636200	MTP DESIGNER TRIAL	< 1.3.3	
1153509	EV Charging Suite 5 Charge Points (EV-CC-S-SUITE-CP5)	< 1.7.1	
1153508	EV Charging Suite 20 Charge Points (EV-CC-S-SUITE-CP20)	< 1.7.1	
1128335	EV Charging Suite 50 Charge Points (EV-CC-S-SUITE-OEM)	< 1.7.1	
1086929	EV Charging Suite 10 Charge Points (EV-CC-S-SUITE-CP10)	< 1.7.1	
1086921	EV Charging Suite 30 Charge Points (EV-CC-S-SUITE-CP30)	< 1.7.1	
1086920	EV Charging Suite 50 Charge Points (EV-CC-S-SUITE-CP50)	< 1.7.1	
1083065	IOL Conf	< 1.7.0.169	

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)
- Vector Informatik GmbH, Andrew Teylu for Reporting.
- Shelltrail AB, Andreas Vikerup for Reporting (see: https://shelltrail.com/research/local-privilege-escalation-to-system-in-wibu-systems-codemeter-application)

Phoenix Contact GmbH & Co. KG

Namespace: https://phoenixcontact.com/psirt

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

psirt@phoenixcontact.com

References

- PCSA-2026-00013 (EXTERNAL): https://phoenixcontact.com/psirt
- Phoenix Contact advisory overview at CERT@VDE (EXTERNAL): https://certvde.com/de/advisories/vendor/phoenixcontact
- VDE-2026-098: Phoenix Contact: CodeMeter Runtime Security Vulnerabilities in License Validation for SW Tools - HTML (SELF): https://certvde.com/en/advisories/vde-2026-098
- VDE-2026-098: Phoenix Contact: CodeMeter Runtime Security Vulnerabilities in License Validation for SW Tools - CSAF (SELF): https://phoenixcontact.csaf-tp.certvde.com/.well-known/csaf/white/2026/vde-2026-098.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
Activation Wizard < 1.8.2	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:H/A:L	8.6
PLCnext Engineer < 2026.0.5 LTS	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:H/A:L	8.6
PLCnext Engineer EDU LIC < 2026.0.5 LTS	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:H/A:L	8.6
FL Network Manager 0.0 - 10.0	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:H/A:L	8.6
MTP DESIGNER < 1.3.3	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:H/A:L	8.6
MTP DESIGNER TRIAL < 1.3.3	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:H/A:L	8.6
CLIPX ENGINEER ASSEMBLE < 1.3.1	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:H/A:L	8.6
MLnext Creation < 2026.12	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:H/A:L	8.6
IO-Link ENGINEER < 6.0.1.11090	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:H/A:L	8.6
MARKING system < 1.3	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:H/A:L	8.6
EV Charging Suite 20 Charge Points (EV-CC-S-SUITE-CP20) <	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:H/A:	8.6

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

Product	CVSS-Vector	CVSS Base Score
1.7.1	L	
EV Charging Suite 50 Charge Points (EV-CC-S-SUITE-OEM) < 1.7.1	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:H/A:L	8.6
EV Charging Suite 10 Charge Points (EV-CC-S-SUITE-CP10) < 1.7.1	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:H/A:L	8.6
EV Charging Suite 5 Charge Points (EV-CC-S-SUITE-CP5) < 1.7.1	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:H/A:L	8.6
IOL Conf < 1.7.0.169	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:H/A:L	8.6
EV Charging Suite 30 Charge Points (EV-CC-S-SUITE-CP30) < 1.7.1	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:H/A:L	8.6
EV Charging Suite 50 Charge Points (EV-CC-S-SUITE-CP50) < 1.7.1	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:H/A:L	8.6
MLnext Execution < 2026.12	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:H/A:L	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
Activation Wizard < 1.8.2	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:H	8.2
PLCnext Engineer < 2026.0.5 LTS	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:H	8.2
PLCnext Engineer EDU LIC < 2026.0.5 LTS	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:H	8.2
FL Network Manager 0.0 - 10.0	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:H	8.2

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

Product	CVSS-Vector	CVSS Base Score
MTP DESIGNER < 1.3.3	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:H	8.2
MTP DESIGNER TRIAL < 1.3.3	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:H	8.2
CLIPX ENGINEER ASSEMBLE < 1.3.1	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:H	8.2
MLnext Creation < 2026.12	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:H	8.2
IO-Link ENGINEER < 6.0.1.11090	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:H	8.2
MARKING system < 1.3	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:H	8.2
EV Charging Suite 20 Charge Points (EV-CC-S-SUITE-CP20) < 1.7.1	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:H	8.2
EV Charging Suite 50 Charge Points (EV-CC-S-SUITE-OEM) < 1.7.1	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:H	8.2
EV Charging Suite 10 Charge Points (EV-CC-S-SUITE-CP10) < 1.7.1	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:H	8.2
EV Charging Suite 5 Charge Points (EV-CC-S-SUITE-CP5) < 1.7.1	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:H	8.2
IOL Conf < 1.7.0.169	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:H	8.2
EV Charging Suite 30 Charge Points (EV-CC-S-SUITE-CP30) < 1.7.1	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:H	8.2
EV Charging Suite 50 Charge Points (EV-CC-S-SUITE-CP50) < 1.7.1	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:H	8.2
MLnext Execution < 2026.12	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

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

Product status

Known affected

Product	CVSS-Vector	CVSS Base Score
Activation Wizard < 1.8.2	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H	7.5
PLCnext Engineer < 2026.0.5 LTS	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H	7.5
PLCnext Engineer EDU LIC < 2026.0.5 LTS	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H	7.5
FL Network Manager 0.0 - 10.0	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H	7.5
MTP DESIGNER < 1.3.3	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H	7.5
MTP DESIGNER TRIAL < 1.3.3	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H	7.5
CLIPX ENGINEER ASSEMBLE < 1.3.1	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H	7.5
MLnext Creation < 2026.12	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H	7.5
IO-Link ENGINEER < 6.0.1.11090	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H	7.5
MARKING system < 1.3	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H	7.5
EV Charging Suite 20 Charge Points (EV-CC-S-SUITE-CP20) < 1.7.1	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H	7.5
EV Charging Suite 50 Charge Points (EV-CC-S-SUITE-OEM) < 1.7.1	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H	7.5
EV Charging Suite 10 Charge Points (EV-CC-S-SUITE-CP10) < 1.7.1	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H	7.5
EV Charging Suite 5 Charge Points (EV-CC-S-SUITE-CP5) < 1.7.1	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H	7.5
IOL Conf < 1.7.0.169	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H	7.5
EV Charging Suite 30 Charge Points (EV-CC-S-SUITE-CP30) < 1.7.1	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H	7.5
EV Charging Suite 50 Charge Points (EV-CC-S-SUITE-CP50) < 1.7.1	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H	7.5
MLnext Execution < 2026.12	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:	7.5

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

Product	CVSS-Vector	CVSS Base Score
	H	

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

CVE description

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
Activation Wizard < 1.8.2	CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:C/C:H/I:N/A:N	7.7
PLCnext Engineer < 2026.0.5 LTS	CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:C/C:H/I:N/A:N	7.7
PLCnext Engineer EDU LIC < 2026.0.5 LTS	CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:C/C:H/I:N/A:N	7.7
FL Network Manager 0.0 - 10.0	CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:C/C:H/I:N/A:N	7.7
MTP DESIGNER < 1.3.3	CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:C/C:H/I:N/A:N	7.7
MTP DESIGNER TRIAL < 1.3.3	CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:C/C:H/I:N/A:N	7.7
CLIPX ENGINEER ASSEMBLE < 1.3.1	CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:C/C:H/I:N/A:N	7.7
MLnext Creation < 2026.12	CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:C/C:H/I:N/A:N	7.7
IO-Link ENGINEER < 6.0.1.11090	CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:C/C:H/I:N/A:N	7.7
MARKING system < 1.3	CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:C/C:H/I:N/A:N	7.7
EV Charging Suite 20 Charge Points (EV-CC-S-SUITE-CP20) < 1.7.1	CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:C/C:H/I:N/A:N	7.7
EV Charging Suite 50 Charge Points (EV-CC-S-SUITE-OEM) < 1.7.1	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
EV Charging Suite 10 Charge Points (EV-CC-S-SUITE-CP10) < 1.7.1	CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:C/C:H/I:N/A:N	7.7
EV Charging Suite 5 Charge Points (EV-CC-S-SUITE-CP5) < 1.7.1	CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:C/C:H/I:N/A:N	7.7
IOL Conf < 1.7.0.169	CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:C/C:H/I:N/A:N	7.7
EV Charging Suite 30 Charge Points (EV-CC-S-SUITE-CP30) < 1.7.1	CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:C/C:H/I:N/A:N	7.7
EV Charging Suite 50 Charge Points (EV-CC-S-SUITE-CP50) < 1.7.1	CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:C/C:H/I:N/A:N	7.7
MLnext Execution < 2026.12	CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:C/C:H/I:N/A:N	7.7

Local Privilege Escalation in CodeMeter Runtime on Windows (CVE-2026-81572)

CVE description

cmu.exe --create-io --file C: creates a predictable temporary file under C:\CM-Stick. The directory and file paths are not properly checked for NTFS reparse points, such as junctions or symbolic links, before file operations are performed. A local attacker can create a junction at the temporary file that points to an arbitrary system path. Because CodeMeter Runtime runs with System privileges, this could allow arbitrary files to be deleted with System privileges and potentially enable local privilege escalation.

CWE:	CWE-59: Improper Link Resolution Before File Access ('Link Following')

Product status

Known affected

Product	CVSS-Vector	CVSS Base Score
Activation Wizard < 1.8.2	CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H	7.8
PLCnext Engineer < 2026.0.5 LTS	CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H	7.8
PLCnext Engineer EDU LIC < 2026.0.5 LTS	CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H	7.8
FL Network Manager 0.0 - 10.0	CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H	7.8
MTP DESIGNER < 1.3.3	CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H	7.8

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

Product	CVSS-Vector	CVSS Base Score
MTP DESIGNER TRIAL < 1.3.3	CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H	7.8
CLIPX ENGINEER ASSEMBLE < 1.3.1	CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H	7.8
MLnext Creation < 2026.12	CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H	7.8
IO-Link ENGINEER < 6.0.1.11090	CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H	7.8
MARKING system < 1.3	CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H	7.8
EV Charging Suite 20 Charge Points (EV-CC-S-SUITE-CP20) < 1.7.1	CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H	7.8
EV Charging Suite 50 Charge Points (EV-CC-S-SUITE-OEM) < 1.7.1	CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H	7.8
EV Charging Suite 10 Charge Points (EV-CC-S-SUITE-CP10) < 1.7.1	CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H	7.8
EV Charging Suite 5 Charge Points (EV-CC-S-SUITE-CP5) < 1.7.1	CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H	7.8
IOL Conf < 1.7.0.169	CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H	7.8
EV Charging Suite 30 Charge Points (EV-CC-S-SUITE-CP30) < 1.7.1	CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H	7.8
EV Charging Suite 50 Charge Points (EV-CC-S-SUITE-CP50) < 1.7.1	CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H	7.8
MLnext Execution < 2026.12	CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H	7.8

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