VDE-2026-050: Phoenix Contact: PLCnext Firmware Security Issues Related to APPs and Configuration Files

Publisher: Phoenix Contact GmbH & Co. KG	Document category: csaf_security_advisory
Initial release date: Wed May 27 10:00:00 CEST 2026	Engine: 2.5.44
Current release date: Wed May 27 10:00:00 CEST 2026	Build Date: Tue May 12 13:41:00 CEST 2026
Current version: 1.0.0	Status: FINAL
CVSSv3.1 Base Score: 8.8	Severity: High
Original language: en	Language: en-GB
Also referred to: VDE-2026-050, PCSA-2026-00005	

Summary

This advisory addresses security issues in PLCnext firmware versions prior to 2026.0.3 that are related to APP handling and the processing of configuration files. The identified vulnerabilities affect APP installation authenticity as well as the handling of configuration data in writable directories. Successful exploitation may allow authenticated attackers with different privilege levels to compromise integrity, availability, and system security of affected PLCnext Control. Both issues are resolved starting with PLCnext firmware version 2026.0.3.

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

Depending on the vulnerability exploited, an attacker may be able to install manipulated APPs, influence the execution of privileged services through crafted configuration files, or execute unauthorized code with elevated permissions. This may lead to a compromise of integrity and availability of the PLCnext Control. Attack vectors include network-based access via the Web-based Management interface as well as local access by authenticated low-privileged users.

Remediation

Phoenix Contact recommends updating affected devices to PLCnext firmware version 2026.0.3 or later, which addresses all vulnerabilities described in this advisory. If immediate updates are not possible, refer to the CVE-specific mitigation measures described below.

Mitigation

The following mitigation measures are recommended. Depending on the operational environment, one or more of these measures may be applied to reduce risk:

- Install APPs only from trusted sources and manually verify the SHA-256 checksum of the downloaded APP file before installation.
- Restrict access to the Web-based Management interface to authorized users only.
- Use firewall configuration to limit access to management interfaces and required services. Firewall configuration should be used to limit network communication to required services and to supervise execution behavior.
- Protect Engineer credentials and apply strong authentication practices.
- If APP functionality is not required for operation, consider disabling the APP Manager to reduce the attack surface.
- Exploitation of CVE-2025-41670 requires local access to the device; therefore, local access should be restricted to authorized and trusted users only. The device should be operated in a secured and controlled environment to prevent unauthorized local access.
- Enable system wide Syslog Server and check local security notifications to detect unexpected APP installation, execution behavior or abnormal system activity.
- Apply the latest firmware and security updates provided by the vendor

Affected Product(s)

Article	Name	Affected	Fixed
1151412	AXC F 1152	<2026.0.3	2026.0.3
1646469	AXC F 1252	<2026.0.3	2026.0.3
1551772	AXC F 2000 EA	<2026.0.3	2026.0.3
2404267	AXC F 2152	<2026.0.3	2026.0.3
1069208	AXC F 3152	<2026.0.3	2026.0.3
1246285	BPC 9102S	<2026.0.3	2026.0.3
1185423	EPC 1522	<2026.0.3	
1136419	RFC 4072R	<2026.0.3	2026.0.3
1051328	RFC 4072S	<2026.0.3	2026.0.3
1760157	VL3 UPC 2440 EDGE	<2026.0.3	2026.0.3
1737875	VPLCNEXT CONTROL 1000	<2026.0.3	2026.0.3
1738453	VPLCNEXT CONTROL 2000	<2026.0.3	2026.0.3
1738454	VPLCNEXT CONTROL 3000	<2026.0.3	2026.0.3
1751491	VPLCNEXT CONTROL 500	<2026.0.3	2026.0.3

Acknowledgments

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

- CERT@VDE for coordination. (see: https://certvde.com)
- Diego Giubertoni from Nozomi for Reporting

Phoenix Contact GmbH & Co. KG

Namespace: https://phoenixcontact.com/psirt

psirt@phoenixcontact.com

References

- PCSA-2026-00005 (EXTERNAL): https://phoenixcontact.com/psirt
- Phoenix Contact advisory overview at CERT@VDE (EXTERNAL): https://certvde.com/de/advisories/vendor/phoenixcontact
- VDE-2026-050: Phoenix Contact: PLCnext Firmware Security Issues Related to APPs and Configuration Files - HTML (SELF): https://certvde.com/en/advisories/VDE-2026-050
- VDE-2026-050: Phoenix Contact: PLCnext Firmware Security Issues Related to APPs and Configuration Files - CSAF (SELF): https://phoenixcontact.csaf-tp.certvde.com/.well-known/csaf/white/2026/vde-2026-050.json

Revision history

Version	Date of the revision	Summary of the revision
1.0.0	Wed May 27 10:00:00 CEST 2026	Initial

Sharing rules

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

Vulnerability Details

Insufficient Verification of Data Authenticity (CVE-2025-41669)

CVE Description

The Web-based Management allows a remote low privileged Engineer user to install additional APPs on the device downloaded from the PLCnext Store without implementing any data verification mechanism, leading to the capability for an Engineer user to reach arbitrary code execution with root privileges on the PLC device. A successful exploitation may allow to install a manipulated APP package, potentially impacting integrity and availability of the PLCnext Control.

CWE: CWE-347: Improper Verification of Cryptographic Signature

Product status

Known affected

Product	CVSS-Vector	CVSS Base Score
<2026.0.3 installed on AXC F 1152 Order number: 1151412	CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H	8.8
<2026.0.3 installed on AXC F 1252 Order number: 1646469	CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H	8.8
<2026.0.3 installed on AXC F 2000 EA Order number: 1551772	CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H	8.8
<2026.0.3 installed on AXC F 2152 Order number: 2404267	CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H	8.8
<2026.0.3 installed on AXC F 3152 Order number: 1069208	CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H	8.8
<2026.0.3 installed on BPC 9102S Order number: 1246285	CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H	8.8
<2026.0.3 installed on EPC 1522 Order number: 1185423	CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H	8.8
<2026.0.3 installed on RFC 4072R Order number: 1136419	CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H	8.8
<2026.0.3 installed on RFC 4072S Order number: 1051328	CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H	8.8
<2026.0.3 installed on VL3 UPC 2440 EDGE Order number: 1760157	CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H	8.8
<2026.0.3 installed on VPLCNEXT CONTROL 1000 Order number: 1737875	CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H	8.8
<2026.0.3 installed on VPLCNEXT CONTROL 2000 Order number: 1738453	CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H	8.8
<2026.0.3 installed on VPLCNEXT CONTROL 3000 Order number: 1738454	CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H	8.8
<2026.0.3 installed on VPLCNEXT CONTROL 500 Order number: 1751491	CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H	8.8

Fixed

Product
2026.0.3 installed on AXC F 1152 Order number: 1151412 (Download)
2026.0.3 installed on AXC F 1252 Order number: 1646469 (Download)
2026.0.3 installed on AXC F 2000 EA Order number: 1551772 (Download)
2026.0.3 installed on AXC F 2152 Order number: 2404267 (Download)
2026.0.3 installed on AXC F 3152 Order number: 1069208 (Download)
2026.0.3 installed on BPC 9102S Order number: 1246285 (Download)
2026.0.3 installed on RFC 4072R Order number: 1136419 (Download)
2026.0.3 installed on RFC 4072S Order number: 1051328 (Download)
2026.0.3 installed on VL3 UPC 2440 EDGE Order number: 1760157 (Download)
2026.0.3 installed on VPLCNEXT CONTROL 1000 Order number: 1737875 (Download)
2026.0.3 installed on VPLCNEXT CONTROL 2000 Order number: 1738453 (Download)
2026.0.3 installed on VPLCNEXT CONTROL 3000 Order number: 1738454 (Download)
2026.0.3 installed on VPLCNEXT CONTROL 500 Order number: 1751491 (Download)

References

- CVSS:4.0/AV:N/AC:L/AT:N/PR:L/UI:N/VC:H/VI:H/VA:H/SC:N/SI:N/SA:N - 8.7 / High (EXTERNAL): https://www.first.org/cvss/calculator/4.0#CVSS:4.0/AV:N/AC:L/AT:N/PR:L/UI:N/VC:H/VI:H/VA:H/SC:N/SI:N/

Untrusted Search Path (CVE-2025-41670)

CVE Description

A local user with low privileges may be able to influence the behavior of a privileged system service by manipulating configuration or application-related files located in user-writable areas of the filesystem. The affected service processes data from locations that are not sufficiently protected against modification by low-privileged users. As the service runs with elevated privileges, successful exploitation may result in a local privilege escalation.

CWE:	CWE-427: Uncontrolled Search Path Element

Product status

Known affected

Product	CVSS-Vector	CVSS Base Score
<2026.0.3 installed on AXC F 1152 Order number: 1151412	CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H	7.8
<2026.0.3 installed on AXC F 1252 Order number: 1646469	CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H	7.8
<2026.0.3 installed on AXC F 2000 EA Order number: 1551772	CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H	7.8
<2026.0.3 installed on AXC F 2152 Order number: 2404267	CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H	7.8
<2026.0.3 installed on AXC F 3152 Order number: 1069208	CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H	7.8
<2026.0.3 installed on BPC 9102S Order number: 1246285	CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H	7.8
<2026.0.3 installed on EPC 1522 Order number: 1185423	CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H	7.8
<2026.0.3 installed on RFC 4072R Order number: 1136419	CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H	7.8
<2026.0.3 installed on RFC 4072S Order number: 1051328	CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H	7.8
<2026.0.3 installed on VL3 UPC 2440 EDGE Order number: 1760157	CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H	7.8
<2026.0.3 installed on VPLCNEXT CONTROL 1000 Order number: 1737875	CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H	7.8
<2026.0.3 installed on VPLCNEXT CONTROL 2000 Order number: 1738453	CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H	7.8
<2026.0.3 installed on VPLCNEXT CONTROL 3000 Order number: 1738454	CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H	7.8
<2026.0.3 installed on VPLCNEXT CONTROL 500 Order number: 1751491	CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H	7.8

Fixed

Product
2026.0.3 installed on AXC F 1152 Order number: 1151412 (Download)
2026.0.3 installed on AXC F 1252 Order number: 1646469 (Download)
2026.0.3 installed on AXC F 2000 EA Order number: 1551772 (Download)
2026.0.3 installed on AXC F 2152 Order number: 2404267 (Download)
2026.0.3 installed on AXC F 3152 Order number: 1069208 (Download)
2026.0.3 installed on BPC 9102S Order number: 1246285 (Download)
2026.0.3 installed on EPC 1522 Order number: 1185423 (Download)
2026.0.3 installed on RFC 4072R Order number: 1136419 (Download)
2026.0.3 installed on RFC 4072S Order number: 1051328 (Download)
2026.0.3 installed on VL3 UPC 2440 EDGE Order number: 1760157 (Download)
2026.0.3 installed on VPLCNEXT CONTROL 1000 Order number: 1737875 (Download)
2026.0.3 installed on VPLCNEXT CONTROL 2000 Order number: 1738453 (Download)
2026.0.3 installed on VPLCNEXT CONTROL 3000 Order number: 1738454 (Download)
2026.0.3 installed on VPLCNEXT CONTROL 500 Order number: 1751491 (Download)

References

- CVSS:4.0/AV:N/AC:L/AT:N/PR:L/UI:N/VC:H/VI:H/VA:H/SC:N/SI:N/SA:N - 8.5 / High (EXTERNAL): https://www.first.org/cvss/calculator/4.0#CVSS:4.0/AV:N/AC:L/AT:N/PR:L/UI:N/VC:H/VI:H/VA:H/SC:N/SI:N/