

VDE-2025-054: Phoenix Contact: Multiple Vulnerabilities in PLCnext Firmware

Publisher: Phoenix Contact GmbH & Co. KG	Document category: csaf_security_advisory
Initial release date: Tue Jul 08 12:00:00 CEST 2025	Engine: 2.5.28
Current release date: Tue Jul 08 12:00:00 CEST 2025	Build Date: Tue Jun 24 15:05:55 CEST 2025
Current version: 1	Status: FINAL
CVSSv3.1 Base Score: 8.8	Severity: Critical
Original language: en	Language: en-GB
Also referred to: VDE-2025-054, PCSA-2024-00018	

Summary

Multiple vulnerabilities in the PLCnext system allowed low-privileged remote attackers to gain unauthorized access or trigger system reboots by manipulating configuration files and symbolic links. Affected services include watchdog, arp-preinit, and security-profile, potentially exposing critical system files. These issues have been resolved in firmware version 2025.0.2.

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

Availability, integrity, or confidentiality of the PLCnext Control might be compromised by attacks using these vulnerabilities.

Remediation

Update to the latest 2025.0.2 Firmware Release. PHOENIX CONTACT recommends to always use an up-to-date version of the PLCnext Engineer.

Product groups

Affected Products.

- Firmware < 2025.0.2 installed on AXC F 1152
- Firmware < 2025.0.2 installed on AXC F 2152
- Firmware < 2025.0.2 installed on AXC F 3152
- Firmware < 2025.0.2 installed on RFC 4072S
- Firmware < 2025.0.2 installed on BPC 9102S

Fixed Product.

- Firmware 2025.0.2 installed on AXC F 1152
- Firmware 2025.0.2 installed on AXC F 2152
- Firmware 2025.0.2 installed on AXC F 3152
- Firmware 2025.0.2 installed on RFC 4072S
- Firmware 2025.0.2 installed on BPC 9102S

Vulnerabilities

CVE-2025-41665

Vulnerability Description

An low privileged remote attacker can enforce the watchdog of the affected devices to reboot the PLC due to incorrect default permissions of a config file.

CWE: CWE-276: Incorrect Default Permissions

Product status

Known affected

Product	CVSS-Vector	CVSS Base Score
Firmware < 2025.0.2 installed on AXC F 1152 Order number: 1151412	CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H	6.5
Firmware < 2025.0.2 installed on AXC F 2152 Order number: 2404267	CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H	6.5
Firmware < 2025.0.2 installed on AXC F 3152 Order number: 1069208	CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H	6.5
Firmware < 2025.0.2 installed on RFC 4072S Order number: 1051328	CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H	6.5
Firmware < 2025.0.2 installed on BPC 9102S Order number: 1246285	CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H	6.5

Fixed

Product
Firmware 2025.0.2 installed on AXC F 1152 Order number: 1151412 (Download)
Firmware 2025.0.2 installed on AXC F 2152 Order number: 2404267 (Download)
Firmware 2025.0.2 installed on AXC F 3152 Order number: 1069208 (Download)
Firmware 2025.0.2 installed on RFC 4072S Order number: 1051328 (Download)
Firmware 2025.0.2 installed on BPC 9102S Order number: 1246285 (Download)

CVE-2025-41666

Vulnerability Description

A low privileged remote attacker with file access can replace a critical file used by the watchdog to get read, write and execute access to any file on the device after the watchdog has been initialized.

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

Product status

Known affected

Product	CVSS-Vector	CVSS Base Score
Firmware < 2025.0.2 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
Firmware < 2025.0.2 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
Firmware < 2025.0.2 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
Firmware < 2025.0.2 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
Firmware < 2025.0.2 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

Fixed

Product
Firmware 2025.0.2 installed on AXC F 1152 Order number: 1151412 (Download)
Firmware 2025.0.2 installed on AXC F 2152 Order number: 2404267 (Download)
Firmware 2025.0.2 installed on AXC F 3152 Order number: 1069208 (Download)
Firmware 2025.0.2 installed on RFC 4072S Order number: 1051328 (Download)
Firmware 2025.0.2 installed on BPC 9102S Order number: 1246285 (Download)

CVE-2025-41667

Vulnerability Description

A low privileged remote attacker with file access can replace a critical file used by the arp-preinit script to get read, write and execute access to any file on the device.

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

Product status

Known affected

Product	CVSS-Vector	CVSS Base Score
Firmware < 2025.0.2 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
Firmware < 2025.0.2 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
Firmware < 2025.0.2 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
Firmware < 2025.0.2 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
Firmware < 2025.0.2 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

Fixed

Product
Firmware 2025.0.2 installed on AXC F 1152 Order number: 1151412 (Download)
Firmware 2025.0.2 installed on AXC F 2152 Order number: 2404267 (Download)
Firmware 2025.0.2 installed on AXC F 3152 Order number: 1069208 (Download)
Firmware 2025.0.2 installed on RFC 4072S Order number: 1051328 (Download)
Firmware 2025.0.2 installed on BPC 9102S Order number: 1246285 (Download)

CVE-2025-41668

Vulnerability Description

A low privileged remote attacker with file access can replace a critical file or folder used by the service security-profile to get read, write and execute access to any file on the device.

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

Product status

Known affected

Product	CVSS-Vector	CVSS Base Score
Firmware < 2025.0.2 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
Firmware < 2025.0.2 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
Firmware < 2025.0.2 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
Firmware < 2025.0.2 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
Firmware < 2025.0.2 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

Fixed

Product
Firmware 2025.0.2 installed on AXC F 1152 Order number: 1151412 (Download)
Firmware 2025.0.2 installed on AXC F 2152 Order number: 2404267 (Download)
Firmware 2025.0.2 installed on AXC F 3152 Order number: 1069208 (Download)
Firmware 2025.0.2 installed on RFC 4072S Order number: 1051328 (Download)
Firmware 2025.0.2 installed on BPC 9102S Order number: 1246285 (Download)

Acknowledgments

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

- CERT@VDE for coordination. (see: <https://certvde.com>)
- Nozomi for Reporting

Phoenix Contact GmbH & Co. KG

Namespace: <https://phoenixcontact.com/psirt>

<https://phoenixcontact.com/psirt>

References

- PCSA-2024-00018 (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-2025-054: Phoenix Contact: Multiple Vulnerabilities in PLCnext Firmware - HTML (SELF): <https://certvde.com/en/advisories/VDE-2025-054>
- VDE-2025-054: Phoenix Contact: Multiple Vulnerabilities in PLCnext Firmware - CSAF (SELF): <https://phoenixcontact.csaf-tp.certvde.com/.well-known/csaf/white/2025/vde-2025-054.json>

Revision history

Version	Date of the revision	Summary of the revision
1	Tue Jul 08 12:00:00 CEST 2025	Initial

Sharing rules

TLP:WHITE

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