VDE-2025-056: Phoenix Contact: Improper Input Validation Vulnerabilities in PLCnext Firmware

Publisher: Phoenix Contact GmbH & Co. KG	Document category: csaf_security_advisory
Initial release date: Wed Aug 12 10:00:00 CEST 2026	Engine: 2.6.6
Current release date: Wed Aug 12 10:00:00 CEST 2026	Build Date: Wed Jul 29 10:02:59 CEST 2026
Current version: 1.0.0	Status: FINAL
CVSSv3.1 Base Score: 9.8	Severity: Critical
Original language: en	Language: en-GB
Also referred to: VDE-2025-056, PCSA-2025-00009	

Summary

This advisory addresses multiple security vulnerabilities in PLCnext firmware versions prior to 2026.0.3. The vulnerabilities may allow unauthenticated attackers to cause denial of service, trigger unexpected system behavior, or execute unauthorized SQL queries. Successful exploitation could impact the availability, integrity, and confidentiality of affected PLCnext Control devices. All issues are resolved in 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

The reported vulnerabilities allow an unauthenticated remote attacker to cause a denial-of-service condition, trigger unexpected behaviour through a buffer overflow, or execute unauthorized SQL queries against affected PLCnext devices. Successful exploitation could impact the availability, integrity, and confidentiality of the system.

Remediation

Phoenix Contact recommends updating affected devices to PLCnext firmware version 2026.0.3 or later, which addresses all vulnerabilities described in this advisory. EPC 1502 and EPC 1522 are obsolete and will not receive the Fix. Please refer to the "General Recommendation" section of this Advisory to identify possible mitigation measures.

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

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
1839159	BPC 9202S	<2026.0.3	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
1886438	Catan C1	<2026.0.3	2026.0.3
1185416	EPC 1502	<2026.0.3	
1185423	EPC 1522	<2026.0.3	

Acknowledgments

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

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

Phoenix Contact GmbH & Co. KG

Namespace: https://phoenixcontact.com/psirt

psirt@phoenixcontact.com

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

References

- PCSA-2025-00009 (EXTERNAL): https://phoenixcontact.com/psirt
- Phoenix Contact advisory overview at CERT@VDE (EXTERNAL): https://certvde.com/de/advisories/vendor/phoenixcontact
- VDE-2025-056: Phoenix Contact: Improper Input Validation Vulnerabilities in PLCnext Firmware - HTML (SELF): https://certvde.com/en/advisories/vde-2025-056
- VDE-2025-056: Phoenix Contact: Improper Input Validation Vulnerabilities in PLCnext Firmware - CSAF (SELF): https://phoenixcontact.csaf-tp.certvde.com/.well-known/csaf/white/2026/vde-2025-056.json

Revision history

Version	Date of the revision	Summary of the revision
1.0.0	Wed Aug 12 10:00:00 CEST 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

Unauthenticated Buffer Overflow in PROFINET Service (CVE-2025-41769)

CVE Description

The device's PROFINET service is affected by a buffer overflow vulnerability that exists in the default configuration. An unauthenticated remote attacker could exploit this vulnerability to reboot the device or execute arbitrary code.

CWE:	CWE-120: Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')

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:N/UI:N/S:U/C:H/I:H/A:H	9.8
<2026.0.3 installed on AXC F 1252 Order number: 1646469	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H	9.8
<2026.0.3 installed on AXC F 2152 Order number: 2404267	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H	9.8
<2026.0.3 installed on AXC F 3152 Order number: 1069208	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H	9.8
<2026.0.3 installed on BPC 9102S Order number: 1246285	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H	9.8
<2026.0.3 installed on BPC 9202S Order number: 1246285	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H	9.8
<2026.0.3 installed on RFC 4072R Order number: 1136419	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H	9.8
<2026.0.3 installed on RFC 4072S Order number: 1051328	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H	9.8
<2026.0.3 installed on VL3 UPC 2440 EDGE Order number: 1760157	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H	9.8
<2026.0.3 installed on VPLCNEXT CONTROL 1000 Order number: 1737875	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H	9.8
<2026.0.3 installed on VPLCNEXT CONTROL 2000 Order number: 1738453	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H	9.8
<2026.0.3 installed on VPLCNEXT CONTROL 3000 Order number: 1738454	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H	9.8
<2026.0.3 installed on VPLCNEXT CONTROL 500 Order number: 1751491	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H	9.8
<2026.0.3 installed on EPC 1502 Order number: 1185416	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H	9.8
<2026.0.3 installed on EPC 1522 Order number: 1185423	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H	9.8

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

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 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 BPC 9202S 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)

Acknowledgments

- T. Weber from CyberDanube for Reporting.

References

- CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:H/VI:H/VA:H/SC:N/SI:N/SA:N - 9.3 / Critical (EXTERNAL): https://www.first.org/cvss/calculator/4.0#CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:H/VI:H/VA:H/SC:N/SI:N

Unauthenticated Denial of Service (CVE-2025-41770)

CVE Description

An unauthenticated denial-of-service vulnerability in the device's PLCnext Engineer communication interface allow an remote attacker to interrupt access via the client application. Successful exploitation prevents communication until the PLCnext service is manually restarted.

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

CWE: CWE-770: Allocation of Resources Without Limits or Throttling

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:N/UI:N/S:U/C:N/I:N/A:H	7.5
<2026.0.3 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
<2026.0.3 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
<2026.0.3 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
<2026.0.3 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
<2026.0.3 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
<2026.0.3 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
<2026.0.3 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
<2026.0.3 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
<2026.0.3 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
<2026.0.3 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
<2026.0.3 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
<2026.0.3 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
<2026.0.3 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
<2026.0.3 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
<2026.0.3 installed on EPC 1502 Order number: 1185416	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H	7.5
<2026.0.3 installed on EPC 1522 Order number: 1185423	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H	7.5

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

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 BPC 9202S 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)
2026.0.3 installed on Catan C1 Order number: 1886438 (Download)

Acknowledgments

- F. Koroknai from CyberDanube for Reporting.

References

- CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:N/VI:N/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:N/UI:N/VC:N/VI:N/VA:H/SC:N/SI:N

SQL injection (CVE-2025-41771)

CVE Description

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

An authenticated attacker with low privileges can access an endpoint in the controller’s web interface that is vulnerable to SQL injection. The vulnerability affects a SQLite database used only for storing notification messages. Therefore, the impact is limited to the system’s notification functionality.

CWE: CWE-89: Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')

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:N/I:L/A:N	4.3
<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:N/I:L/A:N	4.3
<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:N/I:L/A:N	4.3
<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:N/I:L/A:N	4.3
<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:N/I:L/A:N	4.3
<2026.0.3 installed on BPC 9102S Order number: 1246285	CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:L/A:N	4.3
<2026.0.3 installed on BPC 9202S Order number: 1246285	CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:L/A:N	4.3
<2026.0.3 installed on RFC 4072R Order number: 1136419	CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:L/A:N	4.3
<2026.0.3 installed on RFC 4072S Order number: 1051328	CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:L/A:N	4.3
<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:N/I:L/A:N	4.3
<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:N/I:L/A:N	4.3
<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:N/I:L/A:N	4.3
<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:N/I:L/A:N	4.3
<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:N/I:L/A:N	4.3
<2026.0.3 installed on Catan C1 Order number: 1886438	CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:L/A:N	4.3
<2026.0.3 installed on EPC 1502 Order number: 1185416	CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:L/A:N	4.3
<2026.0.3 installed on EPC 1522 Order number: 1185423	CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:L/A:N	4.3

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

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 BPC 9202S 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)
2026.0.3 installed on Catan C1 Order number: 1886438 (Download)

Acknowledgments

- S. Dietz from CyberDanube for Reporting.

References

- CVSS:4.0/AV:N/AC:L/AT:N/PR:L/UI:N/VC:N/VI:L/VA:N/SC:N/SI:N/SA:N - 5.3 / Medium (EXTERNAL): https://www.first.org/cvss/calculator/4.0#CVSS:4.0/AV:N/AC:L/AT:N/PR:L/UI:N/VC:N/VI:L/VA:N/SC:N/SI:N/

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