

VIRTUAL PLCNEXT CONTROL - CHANGE NOTES

Change Notes for the Virtual PLCnext Control VPLCNEXT CONTROL 1000 VPLCNEXT CONTROL 2000 VPLCNEXT CONTROL 3000

Application note

112226_en_03

© Phoenix Contact 2026-09-17

1 General information

The Virtual PLCnext Control is a software-based virtual control for industrial use, suitable for edge applications and the control and monitoring of machines and processes.

This document contains all changes made between firmware version 2025.0 and the current firmware version of the Virtual PLCnext Control:

- VPLCNEXT CONTROL 1000 (item no. 1737875)
- VPLCNEXT CONTROL 2000 (item no. 1738453)
- VPLCNEXT CONTROL 3000 (item no. 1738454)

Current firmware version: **2026.6.1**

Observe the following general notes:

Toolchain

To be able to use all new functions of a firmware version, always use all elements of the toolchain in the same version. The toolchain includes, for example, PLCnext Engineer, SDK and PLCnext CLI.

Documentation

- Make sure you always use the latest documentation. It can be downloaded at:
VPLC 1000: phoenixcontact.com/product/1737875
VPLC 2000: phoenixcontact.com/product/1738453
VPLC 3000: phoenixcontact.com/product/1738454
- Further information on the PLCnext Runtime and programming can be found under plcnext.help
- Further information on security in the context of PLCnext Technology can be found under security.plcnext.help

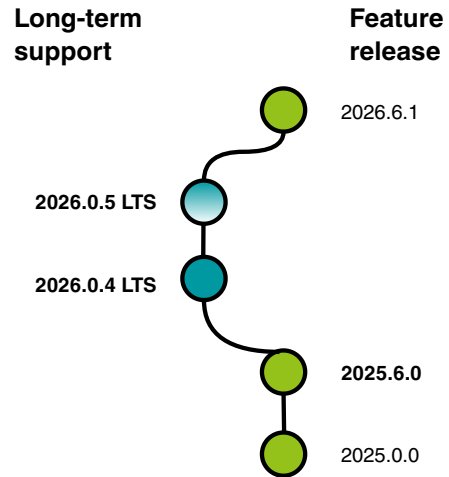
Firmware releases

Feature releases or hotfixes of an LTS version are based on the previous versions of the respective branch. Therefore they only contain the features, changes, error corrections, and security updates of the previous version. Refer to “[Firmware releases VPLCNEXT CONTROL](#)” on page 2 to see on which release branch your firmware version is located and which features, changes, error corrections, and security updates your firmware version contains.

2 Table of contents

1	General information.....	1
2	Table of contents.....	2
3	Firmware releases VPLCNEXT CONTROL	2
4	Changes in firmware version 2026.6.1.....	3
5	Changes in firmware version 2026.0.5 LTS.....	7
6	Changes in firmware version 2026.0.4 LTS.....	8
7	Changes in firmware version 2025.6.0.....	15

3 Firmware releases VPLCNEXT CONTROL



4 Changes in firmware version 2026.6.1

This section describes changes made between firmware version 2026.0.5 LTS and firmware version 2026.6.1. All parts of the previously released version are included in the current version.



To be able to use all new functions of the firmware, you need PLCnext Engineer version 2026.6 or newer.

Select the latest template for firmware version 2026.6 in the PLCnext Engineer project.

4.1 New functions

App Manager

An app (OCI container) may provide one or more web applications. By a reverse proxy configuration defined in `app_info.json`, the web applications are integrated into the host's NGINX server and exposed under dedicated locations such as `/apps/<application name>`.

Linux

The “curl” command-line tool additionally supports the protocols SMTP and SMTPS.

OPC UA

A variable of structured data type is represented as an object in OPC UA server's namespace. The entire structure can be retrieved as a value (so far only each structure member could be accessed).

In order to use this feature, PLCnext Engineer 2026.6 is required, and in the OPC UA configuration the corresponding option needs to be set.

WBM

- At the *Configuration* → *Network* WBM page, the “Advanced configuration” tab has been added. At this tab a hostname can be entered which is stored in the Linux file `/etc/hostname`.
- At the *Configuration* → *Network* WBM page, the “DHCP” option has been added. Note that PROFINET uses the previously configured (static) IP address.

4.2 Changes

Linux

OpenSSL has been updated to version 3.5.

Notification Logger

Additional Security Notifications are emitted:

An “Info” is emitted if the notification archive exceeds 90% of its configured size.

A “Warning” is emitted when old notifications are deleted to reduce its size.

OPC UA

- The logging (“Arp.log”) of the OPC UA has been improved.
- I/O Variables created by a fieldbus which is derived from “Arp::Io::Commons::IoComponentBase” can be represented in the namespace of the OPC UA server.
- When in OPC UA PubSub a reader group with publisher ID “0” is configured, it from now on receives messages from all publisher IDs.

Podman

User rights for the Linux user “admin” are extended. The user can now perform “loginctl” commands including the configuration of lingering.

User Manager

- When logging in via SSH or SFTP Linux interacts with the PLCnext User Manager. This interaction has been reworked. As a consequence, a “reset to factory defaults” must be executed after downgrading from firmware 2026.6 or newer to a firmware 2026.0 LTS or before. Otherwise the user “admin” or any user with the PLCnext role “Admin” cannot login via SSH or SFTP. Logging in via WBM, eHMI, OPC UA or PLCnext Engineer is still possible.
- PLCnext users assigned with the PLCnext role “Admin” can now write via SSH/SFTP to certain directories (e.g. `/opt/plcnext/custom` or `/opt/plcnext/projects/PCWE`). This was possible only for the user “admin” so far.

WBM

The WBM has been optimized for representation on small displays like tablets or mobile phones (responsive web design).

4.3 Error corrections

Apps

Using the file and directory RSC services, a PLCnext Technology App could not read or write files in its data directory (`/opt/plcnext/apps/home/data/<AppId>/`).

Data Logger

When a data logger session is changed (e.g. the set of variables to be recorded was changed), the previously recorded data has been remaining in the database as another table. On rollover this table was copied into the new database file. Consequently, not the entire size of a rollover file could be used. This has been changed.

ESM

When an ESM task causes an exception then the ESM event task “exception” is executed, and after that the ESM event task “stop” is executed. From firmware version 2026.0 LTS, erroneously only the “exception” task was executed. This has been corrected.

GDS

The date and time data types of IEC 61131-3 (i.e. TIME, LTIME, LDATE_AND_TIME, LTIME_OF_DAY) can be connected with signed integer data types of corresponding byte length. In previous firmware versions erroneously a connection to unsigned integer data types was supported. This has been corrected.

IEC 61131-3

When the CPU load was high, the PLC state could change to “Stop | Error | FatalError | Debugging” when attempting to set a code breakpoint using PLCnext Engineer. This has been corrected.

LDAP

After logging in to the WBM, an “500 internal server error” was displayed for users provided by an LDAP server. Nevertheless, the login was successful. This has been corrected.

VPLCnext Control

When the VPLCnext Control has been configured to use certain CPU cores of the host system, an incorrect CPU load could be displayed in WBM or PLCnext Engineer.

4.4 Known limitations and errors

The known limitations and errors can be found in the PLCnext Info Center at:

https://www.plcnext.help/de/known_issues.htm

Here you will find a constantly updated overview of all known issues.

4.5 Security updates

A list of Common Vulnerabilities and Exposures (CVEs) as well as issues that are fixed with this firmware version is published in the **PLCnext Technology – Info Center**. If additional CVEs are published or verified as resolved after the firmware release, they are added to this list accordingly. These updates are marked to ensure transparency and traceability. The list will continuously be maintained and updated.

Please refer to the following link for the most current version of the CVE list:

https://www.plcnext.help/Vulnerabilities_VPLC.htm

For more information about the specified CVE numbers, see:

- <https://nvd.nist.gov/vuln>
- <https://cert.vde.com>

Information on the Phoenix Contact “PSIRT” can be found at: <https://www.phoenixcontact.com/psirt>

Attr

- CVE-2026-54371

Codemeter

The “CodeMeter Runtime” license server was incorrectly active and could be accessed externally.

Curl

- CVE-2026-8286
- CVE-2026-8458
- CVE-2026-8924
- CVE-2026-8926
- CVE-2026-8927
- CVE-2026-8932
- CVE-2026-9079
- CVE-2026-9545
- CVE-2026-9547
- CVE-2026-10536
- CVE-2026-11856
- CVE-2026-12064
- CVE-2026-9080
- CVE-2026-9546
- CVE-2026-11352
- CVE-2026-11586

Expat

- CVE-2026-50219
- CVE-2026-56131
- CVE-2026-56403
- CVE-2026-56404
- CVE-2026-56405
- CVE-2026-56406
- CVE-2026-56407
- CVE-2026-56408
- CVE-2026-56409
- CVE-2026-56410
- CVE-2026-56411
- CVE-2026-56412

Freetype

- CVE-2026-23865

Glibc

- CVE-2026-5450
- CVE-2026-5928

IEC 61131-3

The integrity check of a PLCnext Engineer project has been improved.

Kernel

- CVE-2026-53228
- CVE-2026-53006
- CVE-2026-53002
- CVE-2026-52986
- CVE-2026-46266
- CVE-2026-31682
- CVE-2026-31649
- CVE-2026-31414
- CVE-2026-31402
- CVE-2026-23455
- CVE-2026-43198

Libcap

- CVE-2026-4878

Libcrypt

- CVE-2026-41989

Libpng

- CVE-2026-34757

Libssh

- CVE-2026-0964
- CVE-2026-0965
- CVE-2026-0966
- CVE-2026-0967
- CVE-2026-0968
- CVE-2025-4877

Libssh2

- CVE-2026-7598
- CVE-2026-15661
- CVE-2026-55199
- CVE-2026-55200
- CVE-2026-58050

Libusb

- CVE-2026-23679
- CVE-2026-47104

Ncurses

- CVE-2026-69720

Nfs-utils

- CVE-2026-12801

OpenSSH

- CVE2026-59995
- CVE2026-59996
- CVE2026-59997
- CVE2026-59998
- CVE2026-59999
- CVE2026-60000
- CVE2026-60001
- CVE2026-60002

OpenSSL

A denial-of-service (DoS) vulnerability in former OpenSSL versions allowed a remote, unauthenticated attacker to trigger excessive memory allocation by sending a specially crafted TLS handshake message of only 11 bytes (HollowByte).

Python

- CVE-2026-4519

Python pip

- CVE-2026-1703

Rauc

- CVE-2026-34155

Rsync

- CVE-2026-53791
- CVE-2026-70464
- CVE-2026-70463
- CVE-2026-70461
- CVE-2026-70460
- CVE-2026-70458
- CVE-2026-70456
- CVE-2026-70455
- CVE-2026-70454
- CVE-2026-70453
- CVE-2026-70452
- CVE-2026-53803
- CVE-2026-53802
- CVE-2026-53795
- CVE-2026-53793
- CVE-2026-53790
- CVE-2026-53785
- CVE-2026-53784
- CVE-2026-53783
- CVE-2026-70462
- CVE-2026-70459
- CVE-2026-70457
- CVE-2026-53801
- CVE-2026-53800
- CVE-2026-53799
- CVE-2026-53798
- CVE-2026-53797
- CVE-2026-53796
- CVE-2026-53794
- CVE-2026-53792
- CVE-2026-53789
- CVE-2026-53788
- CVE-2026-53786

Sudo

- CVE-2026-35535

Systemd

- CVE-2026-29111
- CVE-2026-40225

Tar

- CVE-2026-5704

U-boot

- CVE-2026-57256

Util-linux-mount

- CVE-2026-27456

Xz

- CVE-2026-34743

Zlib

- CVE-2026-27171

5 Changes in firmware version 2026.0.5 LTS

This section describes changes made between firmware version 2026.0.4 LTS and firmware version 2026.0.5 LTS. All parts of the previously released version are included in the current version.



To be able to use all new functions of the firmware, you need PLCnext Engineer version 2026.0 LTS or newer.

Select the latest template for firmware version 2026.0 LTS in the PLCnext Engineer project.

5.1 Error corrections

EHMI

A “SIGSEGV” could occur in an eHMI context after executing “Download Changes” (“Write and Start Project Changes” in PLCnext Engineer).

GDS

Forcing of global variables connected to process data items was not possible when the data types differed.

OPC UA

- An invalid “Source-Timestamp” occurred for the “Retain” variable of the OPC UA alarm structure.
- A “SIGSEGV” error could occur between the calls to “DeleteSubscriptions” and “ModifyMonitoredItems” due to a race condition.

WBM

After updating a Chromium-based web browser on the PC the drop-down lists in the WBM could no longer be operated. This has been observed with Microsoft Edge from version 149.0.4022.52 as well as with Google Chrome from version 149.0.7827.54.

This known issue has been fixed.

5.2 Known limitations and errors



The known limitations and errors can be found in the PLCnext Info Center at:

https://www.plcnnext.help/de/known_issues.htm

Here you will find a constantly updated overview of all known issues.

5.3 Security updates

A list of Common Vulnerabilities and Exposures (CVEs) as well as issues that are fixed with this firmware version is published in the **PLCnext Technology – Info Center**. If additional CVEs are published or verified as resolved after

the firmware release, they are added to this list accordingly. These updates are marked to ensure transparency and traceability. The list will continuously be maintained and updated.

Please refer to the following link for the most current version of the CVE list:

https://www.plcnnext.help/Vulnerabilities_VPLC.htm

For more information about the specified CVE numbers, see:

- <https://nvd.nist.gov/vuln>
- <https://cert.vde.com>

Information on the Phoenix Contact “PSIRT” can be found at: <https://www.phoenixcontact.com/psirt>

Gnutls

- CVE-2026-42009

OpenSSL

- CVE-2026-34182
- CVE-2026-7383
- CVE-2026-9076
- CVE-2026-34180
- CVE-2026-45445
- CVE-2026-42766
- CVE-2026-42767
- CVE-2026-45446
- CVE-2026-42770
- CVE-2026-45447

Nginx

- CVE-2026-1642
- CVE-2026-9256

6 Changes in firmware version 2026.0.4 LTS

This section describes changes made between firmware version 2025.6.0 and firmware version 2026.0.4 LTS. All parts of the previously released version are included in the current version.



To be able to use all new functions of the firmware, you need PLCnext Engineer version 2026.0 LTS or newer.

Select the latest template for firmware version 2026.0 LTS in the PLCnext Engineer project.

6.1 New functions

Backup & Restore

The backup file can be encrypted with a password and uploaded to the PC as well as downloaded from the PC. Backup archives can only be restored to that PLC type and firmware version the archive was created with.

DataLogger

Several occurrences of the trigger condition can be recorded in case of a Datalogger session with a trigger condition.

Ethernet/IP

VPLCnext Control devices support the EtherNet/IP slave function (adapter class). This feature can be enabled/disabled via the WBM page "System Services".

PLCnext Apps

- PLCnext Apps can be signed to detect tampering. By default the signature of each installed app is checked at firmware startup. The signature check can be configured at the folder "Configuration" of the WBM page "System - App management". The signature check is enabled by default and Phoenix Contact recommends keeping it enabled. If an app without signature was installed and started before updating the firmware, it is started anyhow. Via WBM it can be stopped and uninstalled but not started again as long as the signature check is active.
- The app part "engineerapp" supports a new Boolean attribute "useAppPersistentDir". For more details refer to the PLCnext Store Info Center. The firmware now supports persistent project data of this app.
- "StrongSwan" can now be controlled from rootless PLCnext Technology Apps.

RSC

- Rework old eCLR remoting services into RSC services to enable secure communication when debugging C# code.
- Introducing a new public RSC service "IVariableBrowseService" that supports browsing all variables:
 - Instance variables (program and component variables)
 - I/O variables provided by pluggable I/O components
- The new RSC service "ISoftwareUpdate" has been implemented.
- New RSC services for PROFINET with the following features:
 - Arp::Io::ProfinetStack::System::Services::IDcpService (Note: only for the interface of the PROFINET controller instance)
 - DCP Scan on the network of a specific interface
 - Edit device parameters (Device Name, IP address, Subnet mask, Standard gateway) - optional remanent or not
 - "Factory Reset" according to PROFINET specification
 - DCP set signal (blinking)
 - Arp::Io::ProfinetStack::System::Services::IAcyclicCommunicationService - PROFINET Implicit Read.

Security

- Security hardening of RSC services.
- UserManager and gRPC provide additional session information:
 - Query/list the roles on the controller
 - List of roles in the current session

VPLCnext Control

Running multiple container instances in one system is supported.

WBM

- A new ESM diagnostics page is implemented. One tab displays ESM statistics and task information and another tab displays a table of ESM exceptions.
- The WBM is extended by the functionality of the "NetNames" tool with a WBM-like user interface. A separate license (<https://www.plcnextstore.com/permalinks/apps/latest/60002172001084>) is required to activate this new functionality. This implementa-

tion adds a “Netnames” tab to the WBM page “PROFINET”. The Netnames functions can be executed via the PROFINET controller network adapter of the PLC.

- The firmware is equipped with the Trust Stores “PLCnext Store Developer” and “PLCnext Store” that contain the necessary certificates to perform the signature check of PLCnext Apps.

6.2 Changes

App

The installation of containerized apps has been optimized to use less memory.

Firewall

The default firewall configuration for outgoing traffic (output rule policy) now allows the connection to the network license server.

SDK and ACF configuration

- Security hardening of process capabilities with the following consequences:
 - When defining processes in the ACF configuration these processes are limited to the capabilities: CAP_NET_BIND_SERVICE, CAP_NET_ADMIN, CAP_NET_RAW, CAP_IPC_LOCK and CAP_SYS_NICE. If a Linux function is used that requires a capability, this capability must be configured using the “name” attribute of the “Process” element in the ACF configuration, too. If this ACF configuration belongs to a PLCnext Technology App, additionally the capabilities CAP_SYS_BOOT and CAP_SYS_TIME can be used. Other Linux capabilities cannot be used.
 - When programming ACF components (either included by /opt/plcnext/projects/Default/Default.acf.config or as part of a PLCnext Technology App) use only such Linux features that are allowed by the Linux capabilities CAP_NET_BIND_SERVICE, CAP_NET_ADMIN, CAP_NET_RAW, CAP_IPC_LOCK or CAP_SYS_NICE. User-defined processes are limited to these capabilities. In case of PLCnext Technology App, additionally the capabilities CAP_SYS_BOOT and CAP_SYS_TIME can be used. In future firmware releases the processes executing these component instances may be restricted further.
 - For security reasons file permissions are restricted and will probably be even more restricted in future firmware versions. Therefore, Phoenix Contact recommends that ACF compo-

nents do write only to files in the folder /opt/plcnext/custom, consider a dedicated subfolder for each component instance. In case of PLCnext Apps writing files shall be limited to folders \$ARP_PATH_APPS_DATA_DIR\$ and \$ARP_PATH_APPS_TEMP_DIR\$.

IEC 61131-3

In combination with PLCnext Engineer 2026.0.1 LTS and newer, the TLS_*_2 function blocks were optimized in terms of real-time and performance.

Licenses

The WIBU CodeMeter Runtime has been updated to version 8.40.

NGINX web server

The Diffie-Hellman groups comply with the recommendation of the German BSI (Bundesamt für Sicherheit in der Informationstechnik).

PLCnext Store

StoreConnector will automatically disconnect after a configurable timespan. Using the WBM, it is also possible to reconnect to the PLCnext Store via internet.

Rest API

The success response for requesting an “access-token” has been extended by an “expires_in” parameter. This parameter indicates the number of seconds after which the session will become invalid if no data request is sent.

System

The timeout for the startup of ACF processes has been increased to 12 seconds. Likewise, the shutdown timeout has been increased to 6 seconds.

6.3 Error corrections

Backup and restore

- A restore of a backup of a PLC project with included “PlcnextBase” library could lead to a crash.
- The system hung when attempting a restore with option “Engineer project” selected although the archive does not contain a PLCnext Engineer project.
- Installed apps were not completely removed when a backup was restored via WBM page “Backup & restore” from an archive that did not contain the installed app.

- Restoring all default configurations to the state after a factory reset of the PLC was not always guaranteed.
- Backup and Restore of the selected “App Data” option did not work for “secure-by-default” devices.

Container apps

The following Known Issue has been fixed:
Re-installation of OCI container apps does not work with Virtual PLCnext Control devices. An error is written to /var/log/syslog “Error: faccessat /opt/plcnext/apps/ mounted/ ... tar.gz: no such file or directory”.
Remedy: After de-installation of the app, first restart the container and thereafter install the app again.

DataLogger

- In case of a DataLogger session with trigger condition, the DataLogger ignored the configured “maxFileSize” and instead used a calculated size. The calculation of this size was wrong. Now the user configured “maxFileSize” is always used.
- If in a DataLogger session with trigger condition a “publishInterval” was configured to a value higher than the cycle time of an ESM cyclic task, incorrect post-cycles could be recorded.
- When several DataLogger sessions with the sink type TSDB were active, a System Watchdog may have occurred because the underlying TSDB data base uses too many file handles (this is indicated in the “Arp.log” file by a lot of “Too many open files” messages).
- Deleting a trigger-based, bounded DataLogger session could cause an exception.

eCLR Runtime

- The PLC system variable “PNIO_DIAG_AVAILABLE” was missing.
- When using curly brackets in the text, the eCLR “Log” class caused an exception.
- The ST code breakpoint handling in combination with programmed loops was not correct.

EHMI

An array defined with a starting index of 1 that is used for eHMI addressing caused a system watchdog. The eHMI array access incorrectly assumed a starting index of 0.

Firewall

- The firmware saves the firewall rules configured via the WBM in an SQL database. Due to a damaged firewall database, the controller became inaccessible via network communication. This damage may have been caused by switching the power supply off and on very

frequently and quickly. To reduce the occurrence of this issue in the future, the code that accesses the firewall database has been optimized. The firewall database now remains closed most of the time and is only opened when required, for example while the firewall is being configured at firmware start or when firewall rules are changed via the WBM.

GDS

- Faulty behavior occurred in case of forcing “IN” variables of a “DI module”: If any variable of a “DI module” was forced to “TRUE”, all other variables were reset to “FALSE”.
- If fieldbus ports were subscribed in a GDS subscription (for example by the DataLogger) and were not unsubscribed when the PLC was shut down, an “Arp::System::Commons::KeyNotFoundException” and, consequently, a System Watchdog occurred. Note: Fieldbus ports can only be added to a GDS subscription from firmware 2025.0 on.
- If a GDS subscription was unsubscribed too soon after its creation (for example before the firmware could internally finish the creation of this subscription), an “Arp::System::Commons::KeyNotFoundException” and, consequently, a System Watchdog occurred.

Logic Analyzer (PLCnext Engineer)

Online values of global variables were displayed incorrectly in the PLCnext Engineer Logic Analyzer.

Modbus client

The usage of function code “FC23” caused a communication error with error code “0x2002”.

OPC UA

No timestamps were generated for OPC UA alarms.

OPC UA server

Due to string processing in logging of OPC UA messages a “SIGSEGV” exception could occur.

PLC

“PLC-RUN” after “PLC-HALT” at a breakpoint did not work for non-“Admin” user roles such as “Engineer” or “Service”.

Proficloud

- The sampling time configured in the WBM for the Proficloud TSD service was not working correctly.

- A “ProfiCloudV3” communication caused a “SigSegV” exception when publishing data during frequent disconnect/reconnect attempts of the connection.

PROFINET

- The local PROFINET stack configuration “PnS.local.config” could be modified without root access.
- A link to the WBM of a device could not be opened in the PN device list of the PROFINET diagnostics.
- In very rare cases, a SIGSEGV may occur in combination with S2 redundancy and an active WBM PROFINET diagnostics page if one of the redundancy controllers experiences connection losses to the PROFINET devices.

SDK

- The firmware can retrieve a “targetIdentifier” for each ACF component, which represents the target of the SDK used to compile that component. This “targetIdentifier” may be incorrect, if it has not been set in the constructor of the related library class by calling the method SetSdkBuildInfo(ARP_VERSION_BUILT, ARP_ABI_VERSION_NAME, ARP_TARGET_IDENTIFIER) of the library base class. This method was introduced with firmware 2026.0 LTS.
Note that for ACF projects created with PLCnext Technology Toolchain 2026.0 and newer, this call will be included in the generated code.
- An attempt to use the RSC service IAppManagerService in C++ resulted in a linker error. As a remedy, the “CMakeLists.txt” had to be extended by the statement “target_link_libraries(\${PROJECT_NAME} PRIVATE Arp.Services.AppManager)” – without a leading “Arp::”.
This known issue has been fixed.

System

- With the Security Profile activated, an unexpected exhaustion of memory resource occurred in small applications using a PROFINET Controller and an active PLCnext Store connection.
- A task watchdog of an EventTask was not handled correctly.
- Sporadically, the firmware executed the “warm restart” event task instead of the “cold restart” task after detecting damage to the retain data. In each case, the retain data was reset to its initial values.

- Sometimes in case of a system watchdog the diagnostic folder of the system monitoring under “/opt/plcnext/logs/Monitoring/Watchdog/” was not synced correctly and some files had no content.
- The custom signal handler in the main process of the firmware incorrectly intercepted fatal signals (e.g. SIGSEGV and SIGKILL replacement paths). This prevented the kernel from generating a core dump for diagnostic purposes.

UM

The API of the “IStatusInfoService” was not publicly available in the SDK.

VPLCnext Control

A network “ping” from the VPLC container to the host system was not possible.

WBM

- The Project Integrity page did not show user changes after a modification. It was unclear whether the new settings had been applied.
- Sometimes buttons overlapped in the “Apps” window.
- System dates around the turn of the year (last days of December or first days of January) were not displayed correctly in the WBM (pages cockpit and date/time).
- The table overview of PROFINET devices in the WBM PROFINET diagnostics incorrectly changed its column width depending on the content to be displayed.
- The “BACK” button on the WBM start page for “Backup & Restore” had no function.
- In the WBM menu for configuring an external SD card, it was not possible to click “CANCEL” if the recovery passwords for the SD card to be encrypted did not match.
- If the “Password ruleset” was changed from “Admin rules” to “Default rules” in the “PASSWORD POLICY” tab, “Unsaved changes” was incorrectly displayed.
- The workflow of changing the default password was incorrect. The explanation in the dialog was unclear.
- The login to the WBM was not possible when a mobile connection was used (for example LTE).
- The value “0.0.0.0” of a DNS server IP address was not accepted to be a valid value.
- In the “PROFINET diagnostics” WBM page, several entries in the status details dialog were incorrectly displayed next to each other instead of one below the other.
This has been corrected.

- Depending on the width of the browser’s window, the “Delete” button and the “Fold”/“Unfold” button in the WBM page “App management” overlapped.
- Apps that were restored from an archive via the WBM page “Backup & restore” were not listed at the WBM page “App management” until the PLC was rebooted.
- If attempting to perform the offline activation of a license via WBM page “License management” with the option “Basic file format” selected, then the button to download the license context file was missing.

6.4 Known limitations and errors



The known limitations and errors can be found in the PLCnext Info Center at:

https://www.plcnext.help/en/known_issues.htm

Here you will find a constantly updated overview of all known issues.

6.5 Security updates

The following security updates have been made in this release. For more information about the specified CVE numbers, see:

- <https://nvd.nist.gov/vuln>
- <https://cert.vde.com>

Information on the Phoenix Contact “PSIRT” can be found at: <https://www.phoenixcontact.com/psirt>

ACF

- CVE-2025-41670

App

PLCnext Technology Apps using containers could not access the gRPC interface because the role “app_user” is no longer a member of the “plcnext” group for “secure-by-default” devices.

Backup and Restore

- The certificates from the Identity Store were not saved within a backup file.
- Restoring a manipulated backup file led to an exception and system watchdog.
- During decryption of an encrypted backup, a WBM alert containing internal security-related information was triggered when a user entered an incorrect password.
- During backup creation it was possible to set an encryption password with the length of one character.

Curl

- CVE-2025-14017
- CVE-2025-0167
- CVE-2025-5025
- CVE-2025-15079
- CVE-2025-14819
- CVE-2025-14524
- CVE-2025-10148
- CVE-2025-15224
- CVE-2026-4873
- CVE-2026-5545
- CVE-2026-5773
- CVE-2026-6253
- CVE-2026-6276
- CVE-2026-6429
- CVE-2026-7168
- CVE-2026-1965
- CVE-2026-3783
- CVE-2026-3784

DPKG

- CVE-2025-6297

Expat

- CVE-2026-45186

Git

- CVE-2025-48384

Glib

- CVE-2025-14512
- CVE-2025-13601
- CVE-2025-14087
- CVE-2025-3360
- CVE-2025-4373
- CVE-2025-7039
- CVE-2025-6052

Glibc

- CVE-2025-15281
- CVE-2026-0861
- CVE-2026-0915
- CVE-2025-8058
- CVE-2025-5702
- CVE-2026-4438

- CVE-2026-4437
- CVE-2026-4046
- CVE-2024-2961

Gnutls

- CVE-2025-32989
- CVE-2025-32988
- CVE-2025-32990
- CVE-2025-6395
- CVE-2025-32988
- CVE-2026-3833
- CVE-2026-33845
- CVE-2026-3832
- CVE-2026-42010

GRPC

- CVE-2024-11407
- CVE-2024-7246

Kernel

- CVE-2026-31431
- CVE-2026-43037
- CVE-2026-43038
- CVE-2026-43284
- CVE-2026-46300
- CVE-2026-43186

Libxpat

- CVE-2026-24515
- CVE-2025-59375
- CVE-2026-41080
- CVE-2026-32777
- CVE-2026-32776
- CVE-2026-32778

Libssh

- CVE-2025-8114
- CVE-2025-5351
- CVE-2025-5987
- CVE-2026-3731

Libtasn

- CVE-2025-13151

Libxml

- CVE-2025-7425

Ncurses

- CVE-2025-6141

Nginx

- CVE-2025-23419
- CVE-2025-53859

Nghttp2

- CVE-2026-27135

NTP

Via web-based management service any parameters for the NTP/chrony configuration could be written to the configuration file and applied accordingly.

Openssh

- CVE-2025-61985
- CVE-2025-61984
- CVE-2025-32728
- CVE-2026-35386
- CVE-2026-35385
- CVE-2026-35414
- CVE-2026-35387
- CVE-2026-35388
- Support of the obsolete “+ssh-rsa” algorithm has now been removed. In order to maintain compatibility with older clients, the algorithm was explicitly reactivated in previous updates, despite being communicated as removed.

Openssl

- CVE-2026-22796
- CVE-2026-22795
- CVE-2025-69421
- CVE-2025-69420
- CVE-2025-69419
- CVE-2025-69418
- CVE-2025-68160
- CVE-2025-15467
- CVE-2025-9230
- CVE-2025-9232

- CVE-2026-31790
- CVE-2026-28390
- CVE-2026-28389
- CVE-2026-28388
- CVE-2026-28387
- CVE-2026-31789

OpenVPN

- CVE-2025-13086

PROFINET

A malformed LLDP frame could cause a crash (stack overflow) and potential code execution.

Python

- CVE-2025-13837
- CVE-2025-12084
- CVE-2025-13836

Rapidjson

- CVE-2024-39684

RSC

- A manipulated message interrupted the RSC communication to the PLCnext Engineer. In addition, the internal CPU system load increased up to 100 %.
- Calls to internal RSC services without SecurityStub were allowed if the providing component was running in another process than the RscGateway.

Rsync

- CVE-2025-10158
- CVE-2026-43617
- CVE-2026-45232
- CVE-2026-43619
- CVE-2026-43620
- CVE-2026-41035
- CVE-2026-43618
- CVE-2026-29518

RSC file service

Read/write access to app directories via the RSC service "Read/Write" was denied on "secure-by-default" devices.

System

- CVE-2025-41669
- By activating the remote gRPC server, it was possible to use every available endpoint without authentication. This includes for example reading and writing GDS variables, as well as restarting the device, and processing a factory reset.
- Missing certificates in case of project integrity in the Trust Store Code Signing led to unclear security notifications.
- Writing primitive variables using "IDataAccessService::Write" instead of "IDataAccessService::WriteSingle", the additional information "from <oldValue> to <newValue>" was missing in the corresponding security notification.
- The AppManager did not lock the loading of an app in time to prevent the PlcManager from loading the eCLR project. This led to an impairment of cybersecurity, as the loaded code could still be executed in the event of an expired license.
- A standard user on the device was able to access any files on the device. This situation was caused by mis-configured sudo permissions associated with the "nft" binary.
- In case of user handling some notifications showed internal user-related information.

Systemd

- CVE-2026-40226

Sqlite

- CVE-2025-6965
- CVE-2025-7709
- CVE-2025-52099

WBM

- CVE-2025-41771
- The WBM certificate management was unable to add PEM certificates which contained "CRLF" instead of "LF".
- In LDAP/LDAPs WBM configuration, a port setting was not reset to default if the port was removed on existing configurations.
- In connection with certificate management, security notifications were not generated anymore.

7 Changes in firmware version 2025.6.0

This section describes changes made between firmware version 2025.0.0 and firmware version 2025.6.0. All parts of the previously released version are included in the current version.

This section describes changes made between firmware version 2025.0.3 and firmware version 2025.6.0. All parts of the previously released version are included in the current version.



To be able to use all new functions of the firmware, you need PLCnext Engineer version 2025.6 or newer. Select the latest template for firmware version 2025.6 in the PLCnext Engineer project.

7.1 New functions

Virtual PLCnext Control

When restarting the virtual PLC via the RSC service (e.g. using WBM or PLCnext Engineer), previously only the PLCnext firmware was restarted. With firmware 2025.6, the Podman container is now restarted.

7.2 Error corrections

App

- If an OCI container app was updated while it was in the RUN state, the app disappeared from the web-based management 2 (WBM 2) without an error message. After restarting the PLC, the app was displayed again. To prevent this behavior, the app had to be set to the STOP state before updating. This known issue has been fixed.
- When installing an app that contains an EHMI part, this EHMI can only be accessed after the Virtual PLCnext Control container has been restarted via its host.

Backup

The backup and restore feature did use a maximum file name length of 256 bytes for the backup archive. In some cases this was too short and backup and restore did not work properly. The maximum file name size has been increased to 4096 bytes.

C/C++

Using the ANSI C API it was possible to trigger a Start() at the PlcManager while the PLC was in state "Starting". This led to an invalid PlcState "Running | Starting". Now the

PlcManager waits until the "Starting" state has been finished.

WBM

- On the "password policy" tab of the WBM page "User policies" the values of the password interval rules "Password changes per interval" and "password change interval" were swapped with firmware version 2025.0.
- On the WBM page "Diagnostics - Profinet", the scrolling behavior has been corrected in the tree view.

OPC UA server

If the OPC UA server's endpoint has been configured with an IP address that does not match to the IP configuration of the PLC, the OPC UA server threw an exception and the firmware exited. In this situation now the OPC UA server emits the notification `Arp.Services.OpcUAServer.StartFailed`. The firmware starts up and after correction of the endpoint configuration a project download turns the OPC UA server into operation.

OPC UA client

The behavior of the PLC's built-in OPC UA client has been improved for a better coherency in the following cases:

- A value change at the server side could be missed by OPC UA client if this change occurred while the connection between client and server is cut.
- After the PLC program is started (also if "Write and start project" is executed in PLCnext Engineer) the OPC UA client now retrieves the latest values from the configured server. After receiving these values, which may take some time, the OPC UA client writes them to the configured variables (thus overwriting the variables' initial value).

System

- If with firmware 2025.0 the static logger was used by a component, which was executed in the PLCnext firmware process, no messages have been logged. This error has been fixed.
- When activating the Security Profile, the IP configuration sometimes got lost and the PLC started with the default IP configuration. The PLC needed to be rebooted another time. This known issue has been fixed.

Proficloud

If too many OUT port variables have been marked as "IoT" in PLCnext Engineer or as "Proficloud" attribute in C++, a System Watchdog (SWD) occurred. With firmware 2025.6,

no SWD occurs in this case. Instead, a warning is issued in the “Arp.log” file, indicating that not all variables are sent to the Proficloud or to an MQTT broker.

Virtual PLCnext Control

- Software watchdogs (SWD) could cause reboot loops. The System Monitoring now prevents these loops.
- The RSC method
IDeviceControlService::ResetToFactoryDefaults()
previously stopped the PLC but did not perform the requested reset. Since this reset is not permitted for Virtual PLCnext Control, the method now has no effect when executed.
Note: This RSC method is also used by PLCnext Engineer.
- When the container is restarted or the host system is rebooted, the folder /var/tmp/ is now cleared.

EHMI

When retrieving a range of array values via REST call, the entire array was returned. This issue has been fixed and now only the values within the requested range are returned.

7.3 Known limitations and errors



The known limitations and errors can be found in the PLCnext Info Center at:
https://www.plcnext.help/en/known_issues.htm
Here you will find a constantly updated overview of all known issues.

7.4 Security updates

The following security updates have been made in this release. For more information about the specified CVE numbers, see:

- <https://nvd.nist.gov/vuln>
- <https://cert.vde.com>

Information on the Phoenix Contact “PSIRT” can be found at: <https://www.phoenixcontact.com/psirt>

Abseil CPP

- CVE-2025-0838

Curl

- CVE-2025-4947

FastCGI

- CVE-2025-23016

Git

- CVE-2025-46835
- CVE-2025-48384
- CVE-2025-48385
- CVE-2025-48386

Less

- CVE-2024-32487

Libxml2

- CVE-2025-6021
- CVE-2025-49794
- CVE-2025-49795
- CVE-2025-49796

Libssh

- CVE-2025-5318

Libpam

- CVE-2025-6020
- CVE-2024-10041

OpenVPN

- CVE-2025-2704

Perl

- CVE-2024-56406

Podman

- CVE-2024-11218
- CVE-2025-6032

Setuptools

- CVE-2025-47273

Sqlite

- CVE-2025-29088
- CVE-2025-29087
- CVE-2025-3277

Sudo

- CVE-2025-32462
- CVE-2025-32463

Syslog-ng

- CVE-2024-47619

TPM2

- CVE-2024-29040

WBM

- With firmware 2025.0, the user role “SecurityAdmin” has been renamed to “SecurityEngineer” but the permissions stayed the same. With that release, a minor issue is present: The “SecurityEngineer” user role must be used together with the “Admin” user role, because the user role “SecurityEngineer” incorrectly had no access rights for the user management as well as to activate/deactivate system services via WBM. This known issue has been fixed.

Container

OCI container applications did not work in “Virtual PLCnext Control”. Container Apps can now be used. An additional configuration is necessary for rootless container networking: /dev/net/tun has to be mounted and /proc/* needs to be unmasked. This is only necessary if container apps are to be used.

PROFINET

A specific invalid UDP datagram sent to a PROFINET UDP port could cause a segmentation fault (SIGSEGV).