CODESYS Control V3 - Insecure default permissions

CODESYS Security Advisory 2025-06

Published: 2025-08-04

Last Change: 2025-08-04

Identifiers, Type and Severity

CVE-2025-41658

CERT@VDE: VDE-2025-049

CODESYS: CDS-93243, RTSL-3062, CDS-93273

CWE-276: Incorrect Default Permissions

CVSS v3.1 Base Score: 5.5 | Medium | CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N

1 Summary

On certain operating systems (e.g., Linux), default file system permissions may allow read access to the files of the CODESYS Control runtime system for non-administrator users. The documentation provided with the CODESYS Runtime Toolkit does not explicitly address this risk. As a result, products based on the toolkit may unintentionally expose sensitive runtime files to local operating system users with limited privileges.

CODESYS Control runtime system based devices are affected if they provide access to the operating system (e.g., via a local user interface or SSH) and user accounts without administrator rights for this access exist or can be created.

2 Affected Products

The following products are affected in all versions before 3.5.21.20.
• CODESYS Runtime Toolkit

The following products are affected in all versions before 4.16.0.0.
• CODESYS Control for BeagleBone SL
• CODESYS Control for emPC-A/iMX6 SL
• CODESYS Control for IOT2000 SL
• CODESYS Control for Linux ARM SL
• CODESYS Control for Linux SL
• CODESYS Control for PFC100 SL
• CODESYS Control for PFC200 SL
• CODESYS Control for PLCnext SL
• CODESYS Control for Raspberry Pi SL
• CODESYS Control for WAGO Touch Panels 600 SL
• CODESYS Virtual Control SL

3 Impact

The affected products do not explicitly restrict read permissions for other local operating system users, potentially allowing unauthorized access to sensitive runtime files.

4 Remediation

Version 3.5.21.20 of the following product provides an updated CODESYS Control V3 Runtime System Documentation:
• CODESYS Runtime Toolkit

In particular, Chapter 5 (Architecture Manual), Section 5.4 (Portings), Subsection 5.4.1 (Security Considerations), Subsection 5.4.1.1 (Operating System Folder Permissions) now provides detailed guidance for device manufacturers on how to address the described security vulnerability. The same information is also included as Mitigation in this advisory.

CODESYS GmbH strongly recommends that this guidance be followed in order to effectively close the security vulnerability on affected devices. Devices are particularly at risk if they offer direct access to the operating system (e.g., via a local user interface or SSH) in combination with the presence or possibility of creating non-administrator user accounts for such access.

Important: Updating the toolkit is not sufficient. For affected customer devices based on the CODESYS Runtime Toolkit the vulnerability needs to be resolved following the instructions in the mentioned documentation.

Update the following products to version 4.16.0.0.
• CODESYS Control for BeagleBone SL
• CODESYS Control for emPC-A/iMX6 SL

• CODESYS Control for IOT2000 SL
• CODESYS Control for Linux ARM SL
• CODESYS Control for Linux SL
• CODESYS Control for PFC100 SL
• CODESYS Control for PFC200 SL
• CODESYS Control for Raspberry Pi SL
• CODESYS Control for WAGO Touch Panels 600 SL
• CODESYS Virtual Control SL

For the updated CODESYS Control SL products, CODESYS GmbH has implemented the necessary measures to address the identified security vulnerability. As a result, access to the runtime directories is now restricted to the Linux user account under which the CODESYS Control runtime is executed. Access is explicitly denied to all other non-administrator users.

Note: Administrator users (e.g., root) may still retain access.

The CODESYS Development System and the products available as CODESYS add-ons can be downloaded and installed directly with the CODESYS Installer or be downloaded from the CODESYS Store. Alternatively, as well as for all other products, you will find further information on obtaining the software update in the CODESYS Update area https://www.codesys.com/download/.

For the following product no fix is available.
• CODESYS Control for PLCnext SL

Since there is no fix available for this product, CODESYS GmbH strongly recommends removing all other existing non-administrator users of the operating system and preventing their re-creation in order to neutralize the security vulnerability.

5 Mitigation

If the CODESYS Control runtime system is operated on an operating system with multi-user support, other users may potentially gain access to runtime-related files. Thus, it is essential to configure the storage locations for CODESYS Control runtime files in accordance with the operating system's security best practices. These locations should, by default, restrict access to unauthorized users. If the operating system does not support such access control mechanisms or if implementing them is not feasible, an alternative approach is to explicitly revoke read and write permissions for all non-administrative users on the directories used by the CODESYS Control runtime system.

The following directories must be secured:
• The directory containing configuration files
• The directory containing binary files
• The working directory used by the runtime system

Note: Protecting individual files is not sufficient. The entire directories must be secured to ensure that any files created in the future are also protected.

Alternatively, where applicable, all non-administrative user accounts can be removed from the system, and their re-creation should be prevented. Additionally, it is recommended to disable remote access methods that allow file access (e.g., SSH) wherever possible, in order to reduce the overall attack surface.

Best practice recommendations for Linux and QNX Systems:
• Create a dedicated privileged group for accessing the above-mentioned directories, and add the user account under which the runtime process is executed to this group.
• Set the file system permissions for these directories to deny access to "other" users (e.g., chmod o-rx).
• If access for additional users is required, they can be added to the privileged group as needed.

6 General Security Recommendations

As part of a security strategy, CODESYS GmbH strongly recommends at least the following best-practice defense measures:

• Use controllers and devices only in a protected environment to minimize network exposure and ensure that they are not accessible from outside

• Use firewalls to protect and separate the control system network from other networks

• Activate and apply user management and password features

• Limit the access to both development and control system by physical means, operating system features, etc.

• Use encrypted communication links

• Use VPN (Virtual Private Networks) tunnels if remote access is required

• Protect both development and control system by using up to date virus detecting solutions

For more information and general recommendations for protecting machines and plants, see also the CODESYS Security Whitepaper.

7 Acknowledgments

This issue was reported by Luca Borzacchiello of Nozomi Networks.

Coordination done by CERT@VDE.

CODESYS GmbH thanks all parties involved for their efforts.

8 Further Information

For additional information regarding the CODESYS products, especially the above-mentioned versions, or about the described vulnerability please contact the CODESYS support.

9 Disclaimer

Note: Not all CODESYS features are available in all territories. For more information on geographic restrictions, please contact sales@codesys.com.

10 Bibliography

[1] CERT@VDE: https://cert.vde.com
[2] CODESYS GmbH: CODESYS Security Whitepaper
[3] CODESYS GmbH: Coordinated Disclosure Policy
[4] CODESYS GmbH download area: https://www.codesys.com/download
[5] CODESYS GmbH security information page: https://www.codesys.com/security
[6] CODESYS GmbH support contact site: https://www.codesys.com/support
[7] Common Vulnerabilities and Exposures (CVE): https://cve.mitre.org
[8] Common Weakness Enumeration (CWE): https://cwe.mitre.org
[9] CVSS Calculator: https://www.first.org/cvss/calculator/3.1

The latest version of this document can be found here:

https://www.codesys.com/fileadmin/user_upload/CODESYS_Group/Ecosystem/Up-to-Date/Security/Security-Advisories/Advisory2025-06_CDS-93243.pdf

Change History

Version	Description	Date
1.0	Initial version	2025-08-04