CODESYS Control V3 - Untrusted boot application

CODESYS Security Advisory 2026-02

Published: 2026-03-24

Last Change: 2026-03-24

Identifiers, Type and Severity

CVE-2025-41660
CERT@VDE: VDE-2026-011
CODESYS: CDS-93242

CWE-669: Incorrect Resource Transfer Between Spheres

CVSS v3.1 Base Score: 8.8| High | CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H

1 Summary

The CODESYS Control runtime system provides a user management mechanism with multiple privilege groups. While only the privileged Administrators and Developer groups are intended to load or debug applications on the controller, users in the restricted Service group are allowed to perform maintenance operations, including explicitly replacing the boot application.

In addition to access control, the CODESYS Control runtime system includes an optional application signing feature. When enabled, the controller executes only applications that have been validly signed by authorized developers. However, the CmpApp component of the CODESYS Control runtime systems allows Service-group users to install a new boot application without requiring any cryptographic validation, if the application signing is not enforced.

As a result, users with Service-level privileges can install arbitrary boot applications and gain control over the code executed on the controller.

Note: The user group “Service” is a predefined group within the CODESYS Control runtime system. If additional user groups have been created or if the permissions of predefined groups have been modified, then the term “Service” should be understood as a synonym for all groups and their users with no or only limited access rights to the “PlcLogic” object, in conjunction with “Add/Remove” or “Modify” permissions for the boot application files.

2 Affected Products

The following products are affected in all versions before 3.5.22.0.

- CODESYS Control RTE (SL)
- CODESYS Control RTE (for Beckhoff CX) SL
- CODESYS Control Win (SL)
- CODESYS HMI (SL)
- CODESYS Runtime Toolkit

The following products are affected in all versions before 4.21.0.0.

- 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

Exploitation of this vulnerability may allow an low-priviledged remote attacker to replace the boot application of the CODESYS Control runtime system, enabling unauthorized code execution on the PLC.

4 Remediation

Update the following products to version 3.5.22.0.

- CODESYS Control RTE (SL)
- CODESYS Control RTE (for Beckhoff CX) SL
- CODESYS Control Win (SL)
- CODESYS HMI (SL)
- CODESYS Runtime Toolkit

Update the following products to version 4.21.0.0. The release of this version is expected for Q2 2026.

- 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

As part of the update, a new configuration file is provided that contains the following setting, which configures the behaviour for Service-group users:

[CmpApp]

SECURITY.UnsignedApplicationFileTransfer=DENY

When this configuration file is used, such as during a new installation, the CODESYS Control runtime system is protected by default.

CODESYS Control runtime systems that continue to use an existing configuration will default to the value ALLOW_WITH_WARNING to ensure compatibility. This setting can be changed either through the Device Security Settings dialog in the CODESYS Development System or directly in the configuration file of the CODESYS Control runtime system (CODESYSControl.cfg) by adding the following setting in the section [CmpApp]:

SECURITY.UnsignedApplicationFileTransfer=

The setting supports the following values:

DENY --> Transfer of unsigned applications is blocked (recommended)

ALLOW_WITH_WARNING --> Transfer is permitted and a warning is logged (default for existing installations)

ALLOW --> Transfer of unsigned applications is permitted (not recommended)

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 [4].

5 Mitigation

Without applying the update, the vulnerability can be mitigated by enforcing the use of signed applications through the following setting:
[CmpApp]
SECURITY.EnforceSignedCode=YES

This can be configured either via the Device Security Settings dialog in the CODESYS Development System or directly in the configuration file of the CODESYS Control runtime system (CODESYSControl.cfg). When this option is enabled, the CODESYS Control runtime system loads only trusted and valid signed applications.

Alternatively, all users belonging to the Service group can be removed, or the Service group can be deleted entirely.

If none of the other mitigation options are feasible, the permissions of the Service group can be restricted by adjusting their access rights. For example, removing modify permissions for the Service group on relevant file system objects can prevent the upload of untrusted boot applications. However, such changes must be applied with caution, as they may lead to inconsistent permissions for this user group and result in unexpected operational limitations. Therefore, this approach should only be considered after a careful assessment of the specific situation.

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 CODESYS support.

9 Disclaimer

CODESYS GmbH assumes no liability whatsoever for indirect, collateral, accidental or consequential losses that occur by the distribution and/or use of this document or any losses in connection with the distribution and/or use of this document. All information published in this document is provided on good faith by CODESYS GmbH. Insofar as permissible by law, however, none of this information shall establish any guarantee, commitment or liability on the part of CODESYS GmbH.

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://api-www.codesys.com/fileadmin/user_upload/CODESYS_Group/Ecosystem/Up-to-Date/Security/Security-Advisories/Advisory2026-02_CDS-93242.pdf

Change History

Version	Description	Date
1.0	Initial version	2026-03-24