CODESYS Control V3 - NULL Pointer Dereference

CODESYS Security Advisory 2025-08

Published: 2025-08-04

Last Change: 2025-09-01

Identifiers, Type and Severity

CVE-2025-41691

CERT@VDE: VDE-2025-070

CODESYS: CDS-94690, CDS-94691

CWE-476: NULL Pointer Dereference

CVSS v3.1 Base Score: 7.5 | High | CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H

1 Summary

A vulnerability in the CODESYS Control runtime system's CmpDevice component allows unauthenticated attackers to cause a denial-of-service (DoS) via specially crafted communication requests.

The issue is triggered by a NULL pointer dereference and also affects systems when outdated CODESYS clients attempt to log in.

Only PLCs based on the CODESYS Runtime Toolkit containing the components CmpDevice, CmpAuditLog, and CmpSessionInformation are impacted.

2 Affected Products

The following products are affected in all versions from 3.5.21.10 and before 3.5.21.20.

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

The following products are affected in all versions from 4.16.0.0 and before 4.17.0.0.

- 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 can lead to a denial-of-service (DoS) condition on affected PLCs, disrupting industrial control systems.

4 Remediation

Update the following products to version 3.5.21.20.

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

Update the following products to version 4.17.0.0.

- 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

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/.

5 Mitigation

The vulnerability can be mitigated by restricting the allowed login authentication type "CmpUserMgr/UserLogin_AuthenticationType" to “ONLY_ASYMMETRIC". 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) by adding the following setting:

```
[CmpUserMgr]
SECURITY.UserLogin_AuthenticationType=ONLY_ASYMMETRIC
```

With this configuration in place, both potential attackers and legacy CODESYS protocol clients (prior to version 3.5.16.0) will be blocked from logging in, thereby preventing execution of the vulnerable code path.

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.

Template: templ_tecdoc_en_V3.0.docx

7 Acknowledgments

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://www.codesys.com/fileadmin/user_upload/CODESYS_Group/Ecosystem/Up-to-Date/Security/Security-Advisories/Advisory2025-08_CDS-94690.pdf

Change History

Version	Description	Date
1.0	Initial version	2025-08-04
2.0	Update for SL runtimes available	2025-09-01