CODESYS Control - Linux/QNX SysSocket flaw

CODESYS Security Advisory 2025-09

Published: 2025-12-01

Last Change: 2025-12-01

Identifiers, Type and Severity

CVE-2025-41739

CERT@VDE: VDE-2025-099

CODESYS: CDS-94934, CDS-95030

CWE-125: Out-of-bounds Read

CVSS v3.1 Base Score: 5.9 | Medium | CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:N/A:H

© CODESYS Group

1 Summary

A vulnerability has been identified in the CODESYS Control runtime system, which includes an abstraction layer designed to ensure compatibility across different operating systems. This layer is used both by affected CODESYS products and by applications running on the PLC.

The platform-specific adaptation of this abstraction layer for Linux and QNX contains a flaw in the SysSocket implementation. Due to incorrect internal handling and depending on how the caller interacts with the affected function, the issue can lead to an out-of-bounds read.

An unauthenticated attacker may be able to exploit this vulnerability via socket-based communication, potentially causing a crash of the corresponding communication task. Additionally, also clients such as the PLCHandler running on Linux or QNX may be affected if they connect to a malicious server that triggers the flaw.

Successful exploitation requires the attacker to win a race condition, which increases the complexity of the attack.

Note: All platforms other than Linux and QNX are not affected.

2 Affected Products

The following products are affected in all versions from 3.5.21.0 and before 3.5.21.40.

- CODESYS PLCHandler
- CODESYS Remote Target Visu
- CODESYS Runtime Toolkit

The following products are affected in all versions from 4.15.0.0 and before 4.19.0.0.

- 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 Edge Gateway for Linux
- CODESYS TargetVisu for Linux SL
- CODESYS Virtual Control SL

3 Impact

Exploitation of this vulnerability may result in a denial-of-service (DoS) condition on affected PLCs or communication clients based on the PLCHandler, potentially disrupting the operation or monitoring, of industrial control systems.

Template: templ_tecdoc_en_V3.0.docx

© CODESYS Group

4 Remediation

Update the following products to version 3.5.21.40.

- CODESYS PLCHandler
- CODESYS Remote Target Visu
- CODESYS Runtime Toolkit

Update the following products to version 4.19.0.0. The release of this version is expected for Q1 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 Edge Gateway for Linux
- CODESYS TargetVisu for Linux 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/.

Template: templ_tecdoc_en_V3.0.docx

5 Mitigation

As the flaw resides in the SysSocketSelect() implementation, which has been switched to a poll()-based approach by default since version 3.5.21.0, the following setting can be added to the configuration file of the affected product (e.g., CODESYSControl.cfg) to revert to the select()-based implementation:

```
[SysSocket]
LinuxSelectPoll=1
```

Note: On Linux select() is limited to less than 1024 file descriptors.

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

© CODESYS Group

• 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 ABB AG.

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

Template: templ_tecdoc_en_V3.0.docx

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/Advisory2025-09_CDS-94934.pdf

Change History

Version	Description	Date
1.0	Initial version	2025-12-01

© CODESYS Group

Template: templ_tecdoc_en_V3.0.docx

© CODESYS Group