CODESYS Control - Linux/QNX SysSocket flaw

VDE-2025-099

Last update	01.12.2025 12:00
Published at	01.12.2025 12:00
Vendor(s)	CODESYS GmbH
External ID	Advisory2025-09_VDE-2025-099
CSAF Document	Download ↗

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.

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.

Affected Product(s)

Model no.	Product name	Affected versions
	CODESYS Control for BeagleBone SL	4.15.0.0<4.19.0.0
	CODESYS Control for IOT2000 SL	4.15.0.0<4.19.0.0
	CODESYS Control for Linux ARM SL	4.15.0.0<4.19.0.0
	CODESYS Control for Linux SL	4.15.0.0<4.19.0.0
	CODESYS Control for PFC100 SL	4.15.0.0<4.19.0.0
	CODESYS Control for PFC200 SL	4.15.0.0<4.19.0.0
	CODESYS Control for PLCnext SL	4.15.0.0<4.19.0.0
	CODESYS Control for Raspberry Pi SL	4.15.0.0<4.19.0.0
	CODESYS Control for WAGO Touch Panels 600 SL	4.15.0.0<4.19.0.0
	CODESYS Control for emPC-A/iMX6 SL	4.15.0.0<4.19.0.0
	CODESYS Edge Gateway for Linux	4.15.0.0<4.19.0.0

Model no.	Product name	Affected versions
	CODESYS PLCHandler	3.5.21.0<3.5.21.40
	CODESYS Remote Target Visu	3.5.21.0<3.5.21.40
	CODESYS Runtime Toolkit	3.5.21.0<3.5.21.40
	CODESYS TargetVisu for Linux SL	4.15.0.0<4.19.0.0
	CODESYS Virtual Control SL	4.15.0.0<4.19.0.0

Vulnerabilities

Expand / Collapse all

CVE-2025-41739 5.9

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.

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/**.

Acknowledgments

CODESYS GmbH thanks the following parties for their efforts:

- CERT@VDE for coordination (see https://www.certvde.com ↗)
- ABB AG for reporting

Revision History

Version	Date	Summary
1.0.0	01.12.2025 10:00	Initial revision.

Kontakt

Impressum

Datenschutzerklärung

Datenschutzhinweise

Diese Seite teilen

Mitglied bei