CODESYS Control V3 - OPC UA Stack

CODESYS Security Advisory 2024-03

Published: 2024-07-05

1 Overview

The CODESYS OPC UA stack of the CODESYS Control runtime system may incorrectly calculate the required buffer size for received requests/responses. This can lead to a crash of the CODESYS runtime system during the subsequent initialization of the receive buffer with zero.

2 Affected Products

The following products are affected in all versions before 3.5.20.10.
• CODESYS Control RTE (SL)
• CODESYS Control RTE (for Beckhoff CX) SL
• CODESYS Control Win (SL)
• CODESYS Runtime Toolkit
• CODESYS HMI (SL)

The following products are affected in all versions before 4.12.0.0.
• 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

3 Vulnerability Identifiers, Type and Severity

VDE-2024-026 [1]

CODESYS JIRA: CDS-89519, CDS-89625

CVE-2024-5000 [7]

CWE-131: Incorrect Calculation of Buffer Size [8]

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 [9]

4 Impact

The CODESYS OPC UA stack, implemented by the CmpOPCUAStack component, is an optional part of the CODESYS runtime system. Both the CODESYS OPC UA Server and the CODESYS OPC UA Client of the CODESYS Control runtime system use the CODESYS OPC UA Stack as a common implementation. The OPC UA protocol enables data exchange between the CODESYS runtime system and OPC UA clients such as SCADA or HMIs, or OPC UA servers such as PLCs or other devices.

If a CODESYS runtime system containing the CmpOPCUAStack component receives a specially crafted request/response, the required buffer size in the CODESYS OPC UA server/client may be incorrectly calculated. This can lead to a crash of the CODESYS runtime system during the subsequent initialization of the receive buffer with zero.

An attacker can exploit this vulnerability by using a malicious OPC UA client to send a crafted request to CODESYS products with an affected CODESYS OPC UA server. Conversely, CODESYS products with an affected CODESYS OPC UA client can be crashed if they have connected to a malicious OPC UA server. CODESYS Control runtime systems usually contain both the OPC UA client and the server. The CODESYS HMI only includes the OPC UA client.

5 Remediation

Update the following products to version 3.5.20.10.
• CODESYS Control RTE (SL)
• CODESYS Control RTE (for Beckhoff CX) SL
• CODESYS Control Win (SL)
• CODESYS Runtime Toolkit
• CODESYS HMI (SL)

Update the following products to version 4.12.0.0.
• 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

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 download area [4].

6 Mitigation

Starting from version 3.5.15.0 of the affected products, the incorrect calculation of the buffer size can be avoided if the maximum supported array length of the OPC UA stack of the CODESYS Control runtime system is limited to a value of 10129639 or less.

This can be achieved by adding the following setting in the CODESYS runtime configuration file (e.g. CODESYSControl.cfg):
[CmpOPCUAStack]
Stack.MaxArrayLenth=10129639

7 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 [2].

8 Acknowledgments

This issue was reported by ABB Schweiz AG.

Coordination done by CERT@VDE.

CODESYS GmbH thanks all parties involved for their efforts.

9 Further Information

For additional information regarding the CODESYS products, especially the above-mentioned versions, or about the described vulnerability please contact the CODESYS support team [6].

10 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.

11 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://customers.codesys.com/index.php?eID=dumpFile&t=f&f=18355&token=e3e5a937ce72602bec39718ddc2f4ba6d983ccd1&download=

Change History

Version	Description	Date
1.0	Initial version	2024-05-22
2.0	Software updates available, product name corrected	2024-06-05
3.0	Further software updates available	2024-07-05