CODESYS Control V3

CODESYS Security Advisory 2023-04

Published: 2023-08-03

1 Overview

The CODESYS Control V3 runtime system does not restrict the memory accesses of the PLC application code to the PLC application data and does not sufficiently check the integrity of the application code by default. This could be exploited by authenticated PLC programmers.

2 Affected Products

All versions of the following products are affected:

- CODESYS Control for BeagleBone SL
- CODESYS Control for emPC-A/iMX6 SL
- CODESYS Control for IOT2000 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 Control RTE (SL)
- CODESYS Control RTE (for Beckhoff CX) SL
- CODESYS Control Win (SL)
- CODESYS Control Runtime System Toolkit
- CODESYS HMI (SL)

3 Vulnerability Identifiers, Type and Severity

VDE-2023-025 [1]

CODESYS JIRA: CDS-82457

CVE-2022-4046, CVE-2023-28355 [7]

CWE-119: Improper Restriction of Operations within the Bounds of a Memory Buffer,
CWE-354: Improper Validation of Integrity Check Value [8]

CVSS v3.1 Base Score 8.8 | 6.5 | High | Medium
CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H | CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:H/A:N [9]

4 Impact

The CODESYS Control runtime system enables embedded or PC-based devices to be a programmable industrial controller. Control programs (PLC application code) can access local or remote IOs, communication interfaces such as serial or sockets, or the file system.

CVE-2022-4046:
CWE-119: Improper Restriction of Operations within the Bounds of a Memory Buffer
CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H
In addition to the functionality described above, there are memory access functions that allow the PLC application code to read or write memory. These are not limited to the data memories that are assigned to it or allocated by it. For this reason, the PLC application code can potentially access the entire RAM memory of the CODESYS Control runtime process surrounding it. This could allow PLC programmers who have successfully authenticated themselves at the controller to execute PLC application code that can modify itself or read or write

sensitive data of the CODESYS Control runtime process.

CVE-2023-28355:
CWE-354: Improper Validation of Integrity Check Value
CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:H/A:N
The PLC application code executed by the CODESYS Control Runtime contains a checksum. This enables the CODESYS development system to check at login whether its loaded project matches the PLC application code executed on the controller. This checksum is not sufficient to reliably detect PLC application code that has been modified in memory or boot application files that have been manipulated.

5 Mitigation

To exploit these vulnerabilities, a successful login to the affected product is required. The online user management therefore protects from exploiting these security vulnerabilities.

CODESYS GmbH strongly recommends using the online user management. This not only prevents from downloading malicious code or boot application files, but also suppresses starting, stopping, debugging or other actions on a known working application that could potentially disrupt a machine or system. As of version 3.5.17.0, the online user management is enforced by default.

In addition, the CODESYS Development System and the CODESYS Control runtime system support optional signing and encryption of the application code loaded on the controller. This feature also prevents the loading and execution of untrusted or modified boot files. If the application code security policy is set to "Enforced Signing", a modified or untrusted application will be detected due to a missing signature and will not be loaded and executed.

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 [2].

7 Acknowledgments

This issue was reported by Reid Wightman of Dragos Inc.

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 the CODESYS support team [6].

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 update 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=17764&token=4b2f3cf3a800d076b22f18d49f278bd8883dbd46&download=

Change History

Version	Description	Date
1.0	Initial version	2023-07-20
2.0	CVSS adapted	2023-08-03