Advisory 2023-01

Security update for CODESYS Control V3 file access

Published: 03 April 2023

Version: 3.0
Template: templ_tecdoc_en_V3.0.docx
File name: Advisory2023-01_CDS-81506.docx

CONTENT

1 Affected Products

Affected are all variants of the following CODESYS V3 products that contain both an application management component (CmpApp or CmpAppEmbedded) and the SysFile component in all versions prior to V3.5.19.0, regardless of CPU type or operating system:
- CODESYS Control RTE (SL)
- CODESYS Control RTE (for Beckhoff CX) SL
- CODESYS Control Win (SL)
- CODESYS Runtime Toolkit
- CODESYS Safety SIL2 Runtime Toolkit
- CODESYS Safety SIL2 PSP
- CODESYS HMI (SL)
- CODESYS Development System V3

Note: Within the CODESYS Development System V3, the simulation runtime is affected.

In addition, the following products based on the CODESYS Control V3 Runtime System Toolkit are affected in all versions prior to V4.8.0.0:
- 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

2 Vulnerability overview

2.1 Type

CWE-668: Exposure of Resource to Wrong Sphere [7]

2.2 Management Summary

The control program could utilize this vulnerability to read and modify system files that are not related to the IEC application of the affected products via IEC code libraries for file access.

2.3 References

CVE: CVE-2022-4224 [6]

CODESYS JIRA: CDS-81506

2.4 Severity Rating

CODESYS GmbH has rated this vulnerability as high.

The CVSS v3.1 base score of 8.8 has been assigned. The CVSS vector string is (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H). [8]

3 Vulnerability details

3.1 Detailed Description

The CODESYS Control runtime system enables embedded or PC-based devices to be a programmable industrial controller. Control programs can access local or remote IOs, communication interfaces such as serial ports or sockets, and local system functions such as the file system, the real-time clock and other OS functions. The control program could utilize this vulnerability to read and modify system files that are not related to the IEC application of the affected products via CAA File, SysFile, SysFileAsync, or other IEC file access libraries.

The security fix is mainly to change the default value of the ForceIecFilePath setting to 1 to deny inappropriate access. Therefore, CODESYS Control runtime systems where ForceIecFilePath=1 is already set in the configuration file are not affected by this vulnerability.

Programming the controller is only possible, if the online user management is deactivated/not active or if the attacker has previously successfully authenticated himself at the controller.

3.2 Exploitability

An authenticated PLC programmer could exploit this vulnerability by downloading IEC code for execution.

3.3 Difficulty

An attacker with low skills would be able to exploit this vulnerability.

3.4 Existence of exploit

There are no known public exploits that specifically target this vulnerability in CODESYS products, but some information about the vulnerability is publicly available.

4 Available software updates

CODESYS GmbH has released version V3.5.19.0, which solves the identified security vulnerabilities for the following products:

- CODESYS Control RTE (SL)
- CODESYS Control RTE (for Beckhoff CX) SL
- CODESYS Control Win (SL)
- CODESYS Runtime Toolkit
- CODESYS Safety SIL2 Runtime Toolkit
- CODESYS Safety SIL2 PSP
- CODESYS HMI (SL)
- CODESYS Development System V3

For the below listed products, CODESYS GmbH has released version V4.8.0.0 based on the CODESYS Control V3 Runtime System Toolkit V3.5.19.0:

- 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

The CODESYS Development System and the products available as CODESYS AddOns 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 [3].

Compatibility notes:
To address the vulnerability, the CODESYS Control runtime systems restrict all file accesses from IEC code to the $PlcLogic$/ working directory/ specified IecFilePath folders and its subdirectories by default. The security fix therefore mainly changes the default ForceIecFilePath setting to 1.

If access to directories or files outside the $PlcLogic$/ working directory is required, PLC vendors may grant access through specific runtime system configurations for IecFilePath. In this case, careful threat analysis is advisable. PLC vendors can find details on possible configurations in the CODESYS Control runtime documentation, tutorial "CODESYS Control Filepath & Placeholders".

CODESYS GmbH strongly recommends keeping the new default value for the setting ForceIecFilePath.

5 Further References

See also CODESYS Security Advisory 2022-02. This describes a similar vulnerability related to accessing configuration files by IEC code.

6 Mitigation

CODESYS GmbH recommends using the available software update to fix the vulnerability.

If the software update is not applied, the CODESYS Control runtime systems already support the ForceIecFilePath setting since version V3.5.2.0. As of this version, CODESYS Control runtime systems can be protected with ForceIecFilePath=1. This setting and other configuration options are described in more detail in the CODESYS Control runtime documentation, tutorial "CODESYS Control Filepath & Placeholders".

To exploit this vulnerability, a successful login to the affected product is required to download and execute the malicious application code to the PLC. The online user management of the affected products therefore protects from exploiting these security vulnerabilities.

CODESYS GmbH strongly recommends using the online user management. This not only prevents an attacker from downloading and execute malicious code, but also suppresses start, stop, debug, or other actions on a known working application that could potentially disrupt a machine or system. As of version V3.5.17.0, the online user management is enforced by default.

As part of a security strategy, CODESYS GmbH recommends the following general defense measures to reduce the risk of exploits:

- 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
- Use VPN (Virtual Private Networks) tunnels if remote access is required
- Activate and apply user management and password features
- Use encrypted communication links
- Limit the access to both development and control system by physical means, operating system features, etc.
- 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 [1].

7 Acknowledgments

This issue was reported independently from each other by Franklin Zhao from ELEX FEIGONG RESEARCH INSTITUTE of Elex CyberSecurity, Inc. and Reid Wightman of Dragos.

CODESYS GmbH thanks for reporting following coordinated disclosure. This helps us to improve our products and to protect customers and users.

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 [5].

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.

Bibliography

[1] CODESYS GmbH: CODESYS Security Whitepaper
[2] CODESYS GmbH: Coordinated Disclosure Policy
[3] CODESYS GmbH update area: https://www.codesys.com/download
[4] CODESYS GmbH security information page: https://www.codesys.com/security
[5] CODESYS GmbH support contact site: https://www.codesys.com/support
[6] Common Vulnerabilities and Exposures (CVE): https://cve.mitre.org
[7] Common Weakness Enumeration (CWE): https://cwe.mitre.org
[8] 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=17553&token=cf49757d232ea8021f0c0dd6c65e71ea5942b12d&download=

Change History

Version	Description	Date
1.0	First version	23.02.2023
2.0	Software updates available	08.03.2023
3.0	Further software updates available	03.04.2023

Template: templ_tecdoc_en_V3.0.docx