Advisory 2022-04

Security update for various CODESYS V3 products using the CODESYS communication protocol

Published: 03 November 2022

Version: 4.0
Template: templ_tecdoc_en_V3.0.docx
File name: Advisory2022-04_CDS-78510.docx

CONTENT

1 Affected Products

All variants of the following CODESYS V3 products containing one of the communication components CmpChannelMgr or CmpChannelMgrEmbedded in all versions prior V3.5.18.0 are affected, regardless of the CPU type or operating system:
- CODESYS Control RTE (SL)
- CODESYS Control RTE (for Beckhoff CX) SL
- CODESYS Control Win (SL)
- CODESYS Gateway
- CODESYS Edge Gateway for Windows
- CODESYS HMI (SL)
- CODESYS OPC DA Server SL
- CODESYS PLCHandler
- CODESYS Development System V3
- CODESYS Control Runtime System Toolkit
- CODESYS Embedded Target Visu Toolkit
- CODESYS Remote Target Visu Toolkit

In addition, the following products based on the CODESYS Control V3 Runtime System Toolkit are affected in all versions prior to V4.5.0.0:
- 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
- CODESYS Edge Gateway for Linux

2 Vulnerability overview

2.1 Type

CWE-334: Small Space of Random Values [7]

2.2 Management Summary

CODESYS protocol communication servers generate weak channel IDs, which can be guessed by attackers to disrupt ongoing communication.

2.3 References

CVE: CVE-2022-22517 [6]

CODESYS JIRA: CDS-78510

2.4 Severity Rating

CODESYS GmbH has rated this vulnerability as high.

The CVSS v3.1 base score of 7.5 has been assigned. The CVSS vector string is (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H). [8]

3 Vulnerability details

3.1 Detailed Description

CODESYS products such as CODESYS Control runtime systems contain communication servers for the CODESYS protocol to enable communication with clients like the CODESYS Development System. The channel ID generated by these servers to identify the communication channels is insufficient.

Guessing the channel ID allows attackers to disrupt existing communication by injecting additional packets or to close this channel. Since the overlying session-bound services have additional integrity checks and further own identifiers used for authentication and authorization, injected packets are detected and also lead to the channel being closed.

3.2 Exploitability

This vulnerability could be exploited remotely.

3.3 Difficulty

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

3.4 Existence of exploit

No known public exploits specifically target this vulnerability in CODESYS products.

4 Available software updates

CODESYS GmbH has released version V3.5.18.0, which solves the identified security vulnerability for the following products:

- CODESYS Control RTE (SL)
- CODESYS Control RTE (for Beckhoff CX) SL
- CODESYS Control Win (SL)
- CODESYS Gateway
- CODESYS Edge Gateway for Windows
- CODESYS HMI (SL)
- CODESYS OPC DA Server SL
- CODESYS PLCHandler
- CODESYS Development System V3
- CODESYS Control Runtime System Toolkit
- CODESYS Embedded Target Visu Toolkit
- CODESYS Remote Target Visu Toolkit

For the below listed products, CODESYS GmbH has released version V4.5.0.0 based on the CODESYS Control V3 Runtime System Toolkit V3.5.18.20:

- CODESYS Control for BeagleBone SL
- CODESYS Control for emPC-A/iMX6 SL
- CODESYS Control for Linux SL
- CODESYS Control for PFC100 SL
- CODESYS Control for PFC200 SL
- CODESYS Control for Raspberry Pi SL
- CODESYS Control for WAGO Touch Panels 600 SL
- CODESYS Edge Gateway for Linux

Version V4.5.0.0 was skipped for the following products. Instead, CODESYS GmbH has released version V4.6.0.0 based on the CODESYS Control V3 Runtime System Toolkit V3.5.18.30 to solve the described vulnerability:

- CODESYS Control for IOT2000 SL
- CODESYS Control for PLCnext SL

The CODESYS Development System and the products available as CODESYS AddOns can be downloaded and installed directly with the CODESYS Installer, which is part of the CODESYS Development System as of version V3.5.17.0.

Alternatively, as well as for all other products, you will find further information on obtaining the software update in the CODESYS Update area [3].

To make the fix effective, both the CODESYS protocol server and the client must be updated. So CODESYS GmbH recommends updating all affected products.

Compatibility information for device manufacturers:
The obsolete marked function NetServerGetChannelInfoByIndex() was removed completely, use NetServerGetChannelInfoByIndex3() instead. The interface between the CmpChannelClient, CmpChannelServer/CmpChannelServerEmbedded, CmpChannelMgr/CmpChannelMgrEmbedded components was reworked, especially the L4 packet structures were redesigned.

5 Mitigation

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

Currently, CODESYS GmbH has not identified any specific workarounds for this vulnerability, in case the software update is not applied.

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].

6 Acknowledgments

The vulnerability was discovered by B. Fels and B. Stuber of Robert Bosch GmbH.

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

7 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].

8 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
[9] ICS-CERT: https://ics-cert.us-cert.gov

The latest version of this document can be found here:

https://customers.codesys.com/index.php?eID=dumpFile&t=f&f=17091&token=c450f8bbbd838c647d102f359356386c6ea5aeca&download=

Change History

Version	Description	Date
1.0	First version	24.03.2022
2.0	Software update available	06.04.2022
3.0	Further software update available, non-released product removed from advisory	30.06.2022
4.0	Further software updates available	03.11.2022