Advisory 2022-16

Security update for CODESYS Control V3 communication server

Published: 25 January 2023

Version: 3.0
Template: templ_tecdoc_en_V3.0.docx
File name: Advisory2022-16_CDS-81444.docx

CONTENT

1 Affected Products

All variants of the following CODESYS V3 products containing the component CmpNameServiceServer in all versions prior V3.5.18.40 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 HMI (SL)
• CODESYS Control Runtime System Toolkit

In addition, the following products based on the CODESYS Control V3 Runtime System Toolkit are affected in all versions prior to V4.7.0.0:
• 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-1288: Improper Validation of Consistency within Input [7]

2.2 Management Summary

An authenticated attacker can send a manipulated packet to the PLC and configure an invalid node name to block consecutive logins by node name over the CODESYS communication protocol.

2.3 References

CVE: CVE-2022-22508 [6]

CODESYS JIRA: CDS-81444, CDS-81451

2.4 Severity Rating

CODESYS GmbH has rated this vulnerability as medium.

The CVSS v3.1 base score of 4.3 has been assigned. The CVSS vector string is (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:L). [8]

3 Vulnerability details

3.1 Detailed Description

CODESYS products such as the CODESYS Control runtime systems contain communication servers for the CODESYS protocol to enable communication with clients such as the CODESYS Development System. The CODESYS Control runtime system also provides a network scan functionality to find PLCs and select them in the CODESYS development system communication dialog to log on to the PLC. The network scan information includes the node name of the PLC among other information. An authenticated attacker can send a manipulated packet to the PLC that configures an invalid node name, or may configure it locally in the CODESYS Control configuration file.

As a result, the PLC still appears in the network scan result, but with the invalid node name. For the CODESYS communication protocol, however, such invalid names are not accepted when logging in by name.

Log in via the device address (example: “[056D]”) or via the IP address (example: “192.168.101.109”) of the

PLC is still possible. After successful authentication at a channel opened by these communication options, the node name can be set to a valid/original name.

3.2 Exploitability

This vulnerability could be exploited remotely after successful authentication.

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 V3.5.18.40, 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 HMI (SL)
• CODESYS Control Runtime System Toolkit

For the below listed products, CODESYS GmbH has released version V4.7.0.0 based on the CODESYS Control V3 Runtime System Toolkit V3.5.18.40:
• 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].

5 Mitigation

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

In case the software update is not applied, CODESYS GmbH has not identified a specific workaround that prevents a successfully authenticated user from renaming the PLC to an invalid node name through manually created online requests or invalid configuration settings.

If the node name has been manipulated, it is always possible to log in using the device address (example: “[056D]”) or the IP address (example: “192.168.101.109”). After successful authentication on a channel opened by these communication options, the node name can be set back to a valid/original name.

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

This vulnerability was reported by icsbob.

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=17351&token=a7c02b2825fea2bcaf80c1a8e62097d72ec90f1a&download=

Change History

Version	Description	Date
1.0	First version	23.11.2022
2.0	Software update available	14.12.2022
3.0	Further software updates available	25.01.2023