



## **Advisory 2022-06**

Security update for several CODESYS V3 products containing a CODESYS communication server

Published: 03 November 2022

Version: 4.0

Template: templ\_tecdoc\_en\_V3.0.docx

File name: Advisory2022-06\_CDS-79444.docx

# CONTENT

	Page
<b>1 Affected Products</b>	<b>3</b>
<b>2 Vulnerability overview</b>	<b>3</b>
2.1 Type	3
2.2 Management Summary	3
2.3 References	3
2.4 Severity Rating	3
<b>3 Vulnerability details</b>	<b>3</b>
3.1 Detailed Description	3
3.2 Exploitability	4
3.3 Difficulty	4
3.4 Existence of exploit	4
<b>4 Available software updates</b>	<b>4</b>
<b>5 Mitigation</b>	<b>5</b>
<b>6 Acknowledgments</b>	<b>5</b>
<b>7 Further Information</b>	<b>5</b>
<b>8 Disclaimer</b>	<b>5</b>
<b>Bibliography</b>	<b>6</b>
<b>Change History</b>	<b>6</b>

## 1 Affected Products

All variants of the following CODESYS V3 products containing the communication servers of the CmpTraceMgr or the CmpSettings component 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 Development System V3
- CODESYS Control Runtime System Toolkit
- CODESYS Embedded Target Visu Toolkit
- CODESYS Remote Target Visu Toolkit

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 V4.5.0.0:

- 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-476: NULL Pointer Dereference, CWE-822: Untrusted Pointer Dereference [7]

### 2.2 Management Summary

The CODESYS protocol communication servers allow authenticated manipulated requests to dereference null pointers or provided untrusted pointers.

### 2.3 References

CVE: CVE-2022-22513, CVE-2022-22514 [6]

CODESYS JIRA: CDS-79444, CDS-75358

### 2.4 Severity Rating

CODESYS GmbH has rated this vulnerability as high.

The CVSS v3.1 base score of 7.1 has been assigned. The CVSS vector string is (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:L/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. Such products contain communication servers for the CODESYS protocol to enable communication with clients like the CODESYS Development System. These servers have the following

vulnerabilities:

CVE-2022-22513: CWE-476: NULL Pointer Dereference

CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H

After successful authentication, crafted communication requests can cause a null pointer dereference in the CmpSettings component and lead to a crash of the affected CODESYS products.

CVE-2022-22514: CWE-822: Untrusted Pointer Dereference

CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:L/A:H

After successful authentication, crafted communication requests can force a read or write access to a dereferenced pointer contained in the request. The request is handled in the CmpTraceMgr component of the affected CODESYS products. The accesses can subsequently lead to local overwriting of memory, whereby the attacker can neither gain the values read internally nor control the values to be written. If invalid memory is accessed, this results in a crash.

The crafted requests are only processed by the affected products, if the online user management is deactivated/not active or if the attacker has previously successfully authenticated himself at the device.

### 3.2 Exploitability

These vulnerabilities could be exploited remotely.

### 3.3 Difficulty

An attacker with low skills would be able to exploit these vulnerabilities.

### 3.4 Existence of exploit

No known public exploits specifically target these vulnerabilities in CODESYS products.

## 4 Available software updates

CODESYS GmbH has released version V3.5.18.0, 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 Gateway
- CODESYS Edge Gateway for Windows
- CODESYS HMI (SL)
- 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 vulnerabilities:

- 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].

## 5 Mitigation

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

To exploit these vulnerabilities, a successful login to the affected product is required. The online user management of the affected products therefore protects from exploiting these security vulnerabilities, even in the case that the software update is not applied.

CODESYS GmbH strongly recommends using the online user management. This not only prevents an attacker from sending malicious requests or downloading virulent code, 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 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].

## 6 Acknowledgments

The vulnerability CVE-2022-22514 was discovered by icsbob.

The vulnerability CVE-2022-22513 was found internally by the CODESYS team.

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](mailto: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=17093&token=15cd8424832ea10dcd4873a409a09a539ee381ca&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