Advisory 2023-02

Security update for CODESYS Control V3

Published: 08 March 2023

Version: 2.0
Template: templ_tecdoc_en_V3.0.docx
File name: Advisory2023-02_CDS-82683.docx

CONTENT

1 Affected Products

All variants of the following CODESYS V3 products in all versions prior V3.5.19.0 containing at least one of the components CmpApp, CmpAppBP, CmpAppForce, CmpFiletransfer or CmpTraceMgr 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 Control Runtime System 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-121: Stack-based Buffer Overflow, CWE-787: Out-of-bounds Write, CWE-822: Untrusted Pointer Dereference, CWE-1288: Improper Validation of Consistency within Input [7]

2.2 Management Summary

CODESYS Control V3 runtime systems are affected by several security vulnerabilities in the communication server for the CODESYS protocol. These can be exploited by authenticated attackers.

2.3 References

CVE: CVE-2022-47378, CVE-2022-47379, CVE-2022-47380, CVE-2022-47381, CVE-2022-47382, CVE-2022-47383, CVE-2022-47384, CVE-2022-47385, CVE-2022-47386, CVE-2022-47387, CVE-2022-47388, CVE-2022-47389, CVE-2022-47390, CVE-2022-47392, CVE-2022-47393 [6]

CODESYS JIRA: CDS-82683, CDS-83104

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. 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-2022-47378: CWE-1288: Improper Validation of Consistency within Input
CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H
After successful authentication, specific crafted communication requests with inconsistent content can cause the CmpFiletransfer component to read internally from an invalid address, potentially leading to a denial-of-service condition.

CVE-2022-47379: CWE-787: Out-of-bounds Write
CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H
After successful authentication, specific crafted communication requests can cause the CmpApp component to write attacker-controlled data to memory, which can lead to a denial-of-service condition, memory overwriting, or remote code execution.

CVE-2022-47380, CVE-2022-47381: CWE-121: Stack-based Buffer Overflow
CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H
After successful authentication, specific crafted communication requests can cause the CmpApp component to write attacker-controlled data to stack, which can lead to a denial-of-service condition, memory overwriting, or remote code execution.

CVE-2022-47382, CVE-2022-47383, CVE-2022-47384, CVE-2022-47386, CVE-2022-47387, CVE-2022-47388, CVE-2022-47389, CVE-2022-47390: CWE-121: Stack-based Buffer Overflow
CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H
After successful authentication, specific crafted communication requests can cause the CmpTraceMgr component to write attacker-controlled data to stack, which can lead to a denial-of-service condition, memory overwriting, or remote code execution.

CVE-2022-47385: CWE-121: Stack-based Buffer Overflow
CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H
After successful authentication, specific crafted communication requests can cause the CmpAppForce component to write attacker-controlled data to stack, which can lead to a denial-of-service condition, memory overwriting, or remote code execution.

CVE-2022-47392: CWE-1288: Improper Validation of Consistency within Input
CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H
After successful authentication, specific crafted communication requests with inconsistent content can cause the CmpApp/CmpAppBP/CmpAppForce components to read internally from an invalid address, potentially leading to a denial-of-service condition.

CVE-2022-47393 : CWE-822: Untrusted Pointer Dereference
CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H
After successful authentication, specific crafted communication requests can cause the CmpFiletransfer component to dereference addresses provided by the request for internal read access, which can lead to a denial-of-service situation.

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 V3.5.19.0, 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 Control Runtime System Toolkit
• CODESYS Safety SIL2 Runtime Toolkit
• CODESYS Safety SIL2 PSP
• CODESYS HMI (SL)
• CODESYS Development System V3

For the below listed products, these issues will be fixed by version V4.8.0.0, which is 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 release of version V4.8.0.0 is expected for beginning of April 2023.

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 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

CVE-2022-47378 was discovered by Vladimir Tokarev, Section 52, Azure IoT Security at Microsoft and Ramin Nafisi, MSTIC at Microsoft.

All other vulnerabilities were discovered by Vladimir Tokarev, Section 52, Azure IoT Security at Microsoft.

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

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=17554&token=5444f53b4c90fe37043671a100dffa75305d1825&download=

Change History

Version	Description	Date
1.0	First version	23.02.2023
2.0	Software updates available, acknowledgments updated	08.03.2023