CODESYS Control V3

CODESYS Security Advisory 2023-05

Published: 2023-08-03

1 Overview

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

2 Affected Products

The following products are affected in all versions prior to 3.5.19.20:

- 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.

The following products are affected in all versions prior to 4.10.0.0:

- 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

3 Vulnerability Identifiers, Type and Severity

VDE-2023-019 [1]

CODESYS JIRA: CDS-85189, CDS-85986

CVE-2023-37545, CVE-2023-37546, CVE-2023-37547, CVE-2023-37548, CVE-2023-37549, CVE-2023-37550, CVE-2023-37551, CVE-2023-37552, CVE-2023-37553, CVE-2023-37554, CVE-2023-37555, CVE-2023-37556, CVE-2023-37557, CVE-2023-37558, CVE-2023-37559 [7]

CWE-20: Improper Input Validation,
CWE-552: Files or Directories Accessible to External Parties,
CWE-787: Out-of-bounds Write

CVSS v3.1 Base Score 6.5 | Medium |
CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H | CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:H/A:N [9]

4 Impact

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. The server implementations of CmpApp, CmpAppBP, CmpAppForce have the following vulnerabilities:

CVE-2023-37545, CVE-2023-37546, CVE-2023-37547, CVE-2023-37548, CVE-2023-37549, CVE-2023-37550:

CWE-20: Improper Input Validation

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

After successful authentication as a user, specific crafted communication requests with inconsistent content can cause the CmpApp component to read internally from an invalid address, potentially leading to a denial-of-service condition.

CVE-2023-37551:

CWE-552: Files or Directories Accessible to External Parties

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

After successful authentication as a user, specially crafted communication requests can utilize the CmpApp component to download files with any file extensions to the controller. In contrast to the regular file download via CmpFileTransfer, no filtering of certain file types is performed here. As a result, the integrity of the CODESYS control runtime system may be compromised by the files loaded onto the controller.

CVE-2023-37552, CVE-2023-37553, CVE-2023-37554, CVE-2023-37555, CVE-2023-37556:

CWE-20: Improper Input Validation

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

After successful authentication as a user, specific crafted communication requests with inconsistent content can cause the CmpAppBP component to read internally from an invalid address, potentially leading to a denial-of-service condition.

CVE-2023-37557:

CWE-787: Out-of-bounds Write

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

After successful authentication as a user, specific crafted communication requests can cause the CmpAppBP component to overwrite a heap-based buffer, which can lead to a denial-of-service condition.

CVE-2023-37558, CVE-2023-37559:

CWE-20: Improper Input Validation

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

After successful authentication as a user, specific crafted communication requests with inconsistent content can cause the CmpAppForce component to read internally from an invalid address, potentially leading to a denial-of-service condition.

5 Remediation

Update the following products to version 3.5.19.20.

- 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

Update the following products to version to 4.10.0.0. This version is scheduled for October 2023.
• 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 add-ons 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 [4].

6 Mitigation

To exploit these vulnerabilities, a successful login to the affected product is required. The online user management therefore protects from exploiting these security vulnerabilities.

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 3.5.17.0, the online user management is enforced by default.

7 General Security Recommendations

As part of a security strategy, CODESYS GmbH strongly recommends at least the following best-practice defense measures:

• 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
• Activate and apply user management and password features
• Limit the access to both development and control system by physical means, operating system features, etc.
• Use encrypted communication links
• Use VPN (Virtual Private Networks) tunnels if remote access is required
• 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 [2].

8 Acknowledgments

These vulnerabilities were reported by Vladimir Tokarev, CPS Research, Microsoft Threat Intelligence Community.

Coordination done by CERT@VDE.

CODESYS GmbH thanks all parties involved for their efforts.

9 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 [6].

10 Disclaimer

11 Bibliography

[1] CERT@VDE: https://cert.vde.com
[2] CODESYS GmbH: CODESYS Security Whitepaper
[3] CODESYS GmbH: Coordinated Disclosure Policy
[4] CODESYS GmbH update area: https://www.codesys.com/download
[5] CODESYS GmbH security information page: https://www.codesys.com/security
[6] CODESYS GmbH support contact site: https://www.codesys.com/support
[7] Common Vulnerabilities and Exposures (CVE): https://cve.mitre.org
[8] Common Weakness Enumeration (CWE): https://cwe.mitre.org
[9] 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=17765&token=04e117e1408fdb8e02b4bc821aa3be819668aef4&download=

Change History

Version	Description	Date
1.0	Initial version	2023-07-20
2.0	Software updates available, CWEs and Impact adapted	2023-08-03