CODESYS products containing WIBU CodeMeter Runtime

CODESYS Security Advisory 2023-10

Published: 2023-08-17

1 Overview

Several CODESYS setups contain and install vulnerable versions of the WIBU CodeMeter Runtime.

2 Affected Products

The setups or packages of the below listed CODESYS products contain and install vulnerable versions of the WIBU CodeMeter Runtime.

CODESYS V2:
• CODESYS Development System V2.3 starting from version 2.3.9.45
• CODESYS SP Realtime NT starting from version V2.3.7.25

CODESYS V3:
The following products are concerned in all versions prior to 3.5.19.30:
• CODESYS Control RTE (SL)
• CODESYS Control RTE (for Beckhoff CX) SL
• CODESYS Control Win (SL)
• CODESYS HMI (SL)
• CODESYS Development System
• CODESYS OPC DA Server SL

The following products are concerned in all versions prior to 4.10.0.0:
• CODESYS Control for Linux SL

The CODESYS Runtime Toolkits (V2 and V3) do not include the WIBU CodeMeter Runtime.

3 Vulnerability Identifiers, Type and Severity

VDE-2023-035 [1]

CODESYS JIRA: CDS-86579, RTSL-1789

CVE-2023-3935 [7]

CWE-122: Heap-based Buffer Overflow, CWE-20: Improper Input Validation,
CWE-648: Incorrect Use of Privileged APIs [8]

CVSS v3.1 Base Score 9.0 | Critical | CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:C/C:H/I:H/A:H [9]

4 Impact

The CODESYS Development System is an IEC 61131-3 programming tool for PLCs based on the CODESYS Control runtime system, which enables embedded or PC-based devices to be a programmable industrial controller. All affected CODESYS products install and use the WIBU CodeMeter Runtime for license management. The manufacturer WIBU-SYSTEMS AG has reported a heap buffer overflow vulnerability in the WIBU CodeMeter Runtime, which can potentially lead to a remote code execution.

For more details see the WIBU-SYSTEMS AG Security Advisory WIBU-230704-01 on https://www.wibu.com/support/security-advisories.html.

5 Remediation

Update the following products to version 3.5.19.30. This version is scheduled for end of September 2023.
• CODESYS Control RTE (SL)
• CODESYS Control RTE (for Beckhoff CX) SL
• CODESYS Control Win (SL)
• CODESYS HMI (SL)

• CODESYS Development System
• CODESYS OPC DA Server SL

Update the following products to version to 4.10.0.0. This version is scheduled for October 2023.
• CODESYS Control for Linux SL

For the legacy CODESYS V2 products, no new version is scheduled.

6 Mitigation

WIBU-SYSTEMS AG recommends updating to CodeMeter Runtime version 7.60c to fix the vulnerability.

Until an update is available for the affected CODESYS products or if this is not to be installed, CODESYS GmbH recommends downloading and installing the current CodeMeter Runtime directly from the website of WIBU-SYSTEMS AG (https://www.wibu.com/support/user/user-software.html).

If neither an update of the affected CODESYS products nor an update of the WIBU CodeMeter Runtime can be performed, you may find further mitigations in the Security Advisory WIBU-230704-01 provided by WIBU-SYSTEMS AG (https://www.wibu.com/support/security-advisories.html).

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

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

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.

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=17809&token=c3b4e3ec4956099de26f0c6caf194d1ba341040a&download=

Change History

Version	Description	Date
1.0	Initial version	2023-08-17