Advisory 2020-06

Security update for several CODESYS V2 and V3 products containing WIBU CodeMeter Runtime

Published: 02 October 2020

Version: 3.0
Template: templ_tecdoc_en_V3.0.docx
File name: Advisory2020-06_CDS-71574.docx

CONTENT

1 Affected Products

The setup or packages of following CODESYS products prior version V3.5.16.20 contain and install vulnerable versions of the WIBU CodeMeter Runtime:
• CODESYS Control for Linux SL
• 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

Depending on the included WIBU CodeMeter Runtime version, not all versions of the affected CODESYS products listed above are concerned by all vulnerabilities:

• All CODESYS versions prior V3.5.15.0
  - WIBU CodeMeter Runtime versions before version 6.81
  - affected by all six vulnerabilities

• V3.5.15.x CODESYS versions (V3.5 SP15 including all patches)
  - WIBU CodeMeter Runtime version 6.81
  - affected by CVE-2020-14509, CVE-2020-14515, CVE-2020-14517, CVE-2020-14519, CVE-2020-16233

• V3.5.16.x CODESYS versions prior to V3.5.16.20
  - WIBU CodeMeter Runtime version 7.00a
  - affected by CVE-2020-14509, CVE-2020-14517, CVE-2020-14519, CVE-2020-16233

The WIBU CodeMeter Runtime is also installed as part of legacy CODESYS V2.3 products. The listed CODESYS product versions are affected by all six WIBU CodeMeter Runtime vulnerabilities, as all of the setups contain WIBU CodeMeter Runtimes prior to version 6.81:
• CODESYS Development System V2.3 (versions from V2.3.9.45 up to (including) V2.3.9.62 are affected)
• CODESYS SP Realtime NT (versions from V2.3.7.25 up to (including) V2.3.7.28 are affected)

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

2 Vulnerability overview

2.1 Type

CVE-2020-14509: CWE-805: Buffer Access with Incorrect Length Value
CVE-2020-14513: CWE-20: Improper Input Validation
CVE-2020-14515: CWE-347: Improper Verification of Cryptographic Signature
CVE-2020-14517: CWE-326: Inadequate Encryption Strength
CVE-2020-14519: CWE-346: Origin Validation Error
CVE-2020-16233: CWE-404: Improper Resource Shutdown or Release [7]

2.2 Management Summary

Several CODESYS setups contain and install vulnerable versions of the WIBU CodeMeter Runtime and are affected by their vulnerabilities.

2.3 References

CVE: CVE-2020-14509, CVE-2020-14513, CVE-2020-14515, CVE-2020-14517, CVE-2020-14519, CVE-2020-16233 [6]

CISA (ICS_CERT): ICSA-20-203-01 [9]

WIBU-SYSTEMS AG: WIBU-200521-01, WIBU-200521-02, WIBU-200521-03, WIBU-200521-04, WIBU-200521-05, WIBU-200521-06 (See https://www.wibu.com/support/security-advisories.html)

CODESYS JIRA: CDS-71574, CDS-72324, CDS-72734, CDS-72739, CDS-72923, CDS-72930, LCDS-335, LCDS-336

2.4 Severity Rating

CODESYS GmbH has rated this vulnerability as critical.

The CVSS v3.0 base score of 10.0 has been assigned. The CVSS vector string is (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H). [8]

3 Vulnerability details

3.1 Detailed Description

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 recently published six vulnerabilities regarding the product WIBU CodeMeter Runtime. Successful exploitation of these vulnerabilities could allow an attacker to access heap data, cause a denial-of-service condition, attain remote code execution, alter and forge license files or disturb normal operation of the CODESYS products that utilize the WIBU CodeMeter Runtime.

3.2 Exploitability

This vulnerability could be exploited remotely.

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 these vulnerabilities in CODESYS products.

4 Available software updates

CODESYS GmbH has released the versions below to solve the noted vulnerability issue for all affected CODESYS products by updating the included WIBU CodeMeter Runtime to version 7.10a:

V3.5.16.20:
• CODESYS Control for Linux SL
• 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

V2:
• CODESYS Development System version V2.3.9.63:
• CODESYS SP Realtime NT version V2.3.7.29:

Please visit the CODESYS update area for more information on how to obtain the software updates [3].

5 Mitigation

WIBU-SYSTEMS AG strongly recommends updating to CodeMeter Runtime version 7.10a to fix the vulnerabilities. Following this, CODESYS GmbH suggests using the available updates for the affected CODESYS products, which include the WIBU CodeMeter Runtime version 7.10a.

In case the update of the affected CODESYS products is not applied, CODESYS GmbH recommends downloading and installing the latest CodeMeter Runtime directly from the WIBU-SYSTEMS AG website (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 advisories provided by WIBU-SYSTEMS AG (https://www.wibu.com/support/security-advisories.html).

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
• 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

CODESYS GmbH thanks those in the security community, who help us to improve our products and to protect customers and users through coordinated vulnerability disclosure.

These issues were discovered in WIBU CodeMeter Runtime by Sharon Brizinov and Tal Keren of Claroty. Following the WIBU-SYSTEM AG advisories, CODESYS GmbH found that several CODESYS products are also affected.

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/3.0
[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=13245&token=12e702eb28edb2de082dc2f5e1375bea35c2fd1d&download=

Change History

Version	Description	Date
1.0	First version	16.09.2020
2.0	Software update available	24.09.2020
3.0	Further software update available, affected products more clearly described	02.10.2020