# CODESYS Key

CODESYS Security Advisory 2025-01

Published: 2025-01-21

## 1 Overview

The CODESYS Key USB dongle, which is based on WIBU CodeMeter technology, is affected by a physical side-channel vulnerability.

## 2 Affected Products

CODESYS Keys with serial numbers starting with “3-”, e.g. 3-4380431, and running a firmware version prior to 4.52.

## 3 Vulnerability Identifiers, Type and Severity

VDE-2025-001 [1]

CODESYS JIRA: CDS-91776

CVE-2024-45678 [7]

CWE-203: Observable Discrepancy [8]

CVSS v3.1 Base Score 4.9 | Medium | CVSS:3.1/AV:P/AC:H/PR:N/UI:N/S:C/C:H/I:N/A:N [9]

## 4 Impact

The CODESYS Key is a USB dongle for secure storage of your CODESYS software licenses based on WIBU CodeMeter technology. The manufacturer WIBU-SYSTEMS AG has reported a physical side-channel vulnerability in a cryptographic library from Infineon Technologies that is part of the WIBU CmDongle firmware and thus also in the affected CODESYS Keys.

The exploitation of this vulnerability has been classified as complex. Potential attackers need physical access to the CODESYS Key and special equipment to exploit the vulnerability.

For more details see the WIBU-SYSTEMS AG Security Advisory WIBU-100094 on https://www.wibu.com/support/security-advisories.html.

In addition to licensing, the CODESYS Key can also be used for secure storage of secret data. The identified CVSS is the highest rating that can occur in combination with the various applications in the CODESYS software. If the CODESYS key is also used with applications from other vendors, the rating may differ. In this case, the respective vendor and/or the WIBU-SYSTEMS AG security advisory should be consulted.

## 5 Remediation

Update the CODESYS Key firmware to version 4.52.

Updating the firmware also protects the future usage of additional CODESYS Key features by the CODESYS software and general usage by other software. The update can be installed, for example, via the CodeMeter Control Center.

## 6 Mitigation

Regardless of the vulnerability described here, CODESYS GmbH recommends that physical access to the CODESYS Key should only be granted to authorized persons. Especially in the case of productive control systems, removal of the CODESYS Key can affect the controlled machine or process.

This generally recommended restriction of access also reduces the attack surface for this vulnerability, as its exploitation requires physical access.

## 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

This issue was reported by NinjaLabs.

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 download 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=18751&token=67384bc706d606a395afb3c0a0a794e49cc8d27d&download=

## Change History

| Version | Description | Date |
|---|---|---|
| 1.0 | Initial version | 2025-01-21 |