CODESYS Control V3 web server

CODESYS Security Advisory 2024-05

Published: 2024-09-24

1 Overview

The CODESYS web server component of the CODESYS Control runtime system is used by the CODESYS WebVisu to display visualization screens in a web browser. Receiving a specifically crafted TLS packet on an HTTPS connection causes the CODESYS web server to crash because the return value of an underlying function is not checked correctly for such unusual conditions.

2 Affected Products

The following products are affected in all versions before 3.5.20.30.
• CODESYS Control RTE (SL)
• CODESYS Control RTE (for Beckhoff CX) SL
• CODESYS Control Win (SL)
• CODESYS HMI (SL)
• CODESYS Runtime Toolkit
• CODESYS Embedded Target Visu Toolkit
• CODESYS Remote Target Visu Toolkit

The following products are affected in all versions before 4.14.0.0.
• CODESYS Control for BeagleBone SL
• CODESYS Control for emPC-A/iMX6 SL
• CODESYS Control for IOT2000 SL
• CODESYS Control for Linux ARM 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
• CODESYS Virtual Control SL

3 Vulnerability Identifiers, Type and Severity

VDE-2024-057 [1]

CODESYS JIRA: CDS-89666, CDS-90549

CVE-2024-8175 [7]

CWE-754: Improper Check for Unusual or Exceptional Conditions [8]

CVSS v3.1 Base Score 7.5 | High | CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H [9]

4 Impact

The CODESYS web server, implemented by the CmpWebServer component, is an optional part of the CODESYS Control runtime system. It is used by the CODESYS WebVisu to display CODESYS visualization screens in a web browser. The CODESYS web server supports both the HTTP and HTTPS protocols. Because the CODESYS web server does not correctly check the return value of an underlying function, it reacts in a wrong way to specifically crafted TLS packets that are received via an HTTPS connection. This causes the CODESYS web server to access invalid memory and the web server task to crash.

5 Remediation

Update the following products to version 3.5.20.30.
• CODESYS Control RTE (SL)
• CODESYS Control RTE (for Beckhoff CX) SL
• CODESYS Control Win (SL)

• CODESYS HMI (SL)
• CODESYS Runtime Toolkit
• CODESYS Embedded Target Visu Toolkit
• CODESYS Remote Target Visu Toolkit

Update the following products to version 4.14.0.0.
• CODESYS Control for BeagleBone SL
• CODESYS Control for emPC-A/iMX6 SL
• CODESYS Control for IOT2000 SL
• CODESYS Control for Linux ARM 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
• CODESYS Virtual Control SL

The release of version 4.14.0.0 is expected for end of November 2024.

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 download area [4].

6 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].

7 Acknowledgments

This issue was reported by ABB.

Coordination done by CERT@VDE.

CODESYS GmbH thanks all parties involved for their efforts.

8 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].

9 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.

10 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=18604&token=d5e1e2820ee63077b875b3bb41014b1f102e88a3&download=

Change History

Version	Description	Date
1.0	Initial version	2024-08-29
2.0	Software updates available	2024-09-24