CODESYS Visualization user management bypass in WebVisu

CODESYS Security Advisory 2025-05

Published: 2025-04-24

1 Overview

An unauthenticated attacker can read static visualization files of the CODESYS WebVisu, by bypassing the CODESYS Visualization user management applying forced browsing.

2 Affected Products

The following product is affected in all versions before 4.8.0.0.
• CODESYS Visualization

The following products are affected in all versions before 3.5.21.0.
• 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 4.15.0.0.
• 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-2025-027 [1]

CODESYS JIRA: VIS-5003, CDS-90142

CVE-2025-2595 [7]

CWE-425: Direct Request ('Forced Browsing') [8]

CVSS v3.1 Base Score 5.3 | Medium | CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N [9]

4 Impact

The CODESYS Visualization, together with the CmpWebServer component in the CODESYS Control Runtime, allows users to create browser-based visualizations for monitoring and controlling industrial processes. Access to these visualizations can be restricted using the built-in user management.

However, on CODESYS Control Runtime systems, where an application with a CODESYS WebVisu is executed, an unauthenticated remote attacker can bypass the user management and read visualization files by means of forced browsing. The exposed files, accessible via a web browser, contain only static visualization data such as text lists, icons or images, but no live data from the controlled system.

5 Remediation

Update the following product to version 4.8.0.0.

• CODESYS Visualization

Update the following products to version 3.5.21.0.

• 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 4.15.0.0.

• 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

Updates of both the CODESYS Visualization and the CODESYS Control Runtime System or the CODESYS HMI are required to fix the vulnerability.

Moreover, existing CODESYS projects that include a CODESYS WebVisu must be recompiled and downloaded to the updated HMI or PLC.

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 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 M. Ankith of Honeywell.

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

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://codesys.com/fileadmin/user_upload/CODESYS_Group/Ecosystem/Up-to-Date/Security/Security-Advisories/Advisory2025-05_VIS-5003.pdf

Change History

Version	Description	Date
1.0	Initial version	2025-04-24