CODESYS Control Win and CODESYS (Edge) Gateway for Windows

CODESYS Security Advisory 2024-02

Published: 2024-06-05

1 Overview

All legitimate local Microsoft Windows users can read or modify files that are located in the working directory of the affected CODESYS products, even if they are executed under a different user or in the system context.

2 Affected Products

The following products are affected in all versions prior to 3.5.20.10:
• CODESYS Control Win (SL)
• CODESYS Edge Gateway for Windows
• CODESYS Gateway for Windows
• CODESYS HMI (SL)
• CODESYS Development System V3

Note: Within the CODESYS Development System V3, the simulation runtime is affected.

3 Vulnerability Identifiers, Type and Severity

VDE-2024-027 [1]

CODESYS JIRA: CDS-87336, CDS-89376, CDS-89520, CDS-89168, CDS-89387, CDS-89777

CVE-2023-5751 [7]

CWE-668: Exposure of Resource to Wrong Sphere [8]

CVSS v3.1 Base Score: 7.8 | High | CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H [9]

4 Impact

The CODESYS Development System is an IEC 61131-3 programming tool for the industrial controller and automation technology sector. The integrated runtime for simulating CODESYS projects as well as CODESYS Control Win V3, CODESYS HMI and the CODESYS (Edge) Gateway running under the Microsoft Windows operating system have their working directory under "%ProgramData%\CODESYS\" by default. All legitimate local Microsoft Windows users can read or modify files in this working directory, even if the affected products are running under a different user or in the system context.

5 Remediation

Update the following products to version 3.5.20.10.
• CODESYS Control Win (SL)
• CODESYS Edge Gateway for Windows
• CODESYS Gateway for Windows
• CODESYS HMI (SL)
• CODESYS Development System V3

The working directories of the affected products are moved to "%APPDATA%\CODESYS\", which is usually located in "C:\Users\<user>\AppData\CODESYS\" and can only be accessed by the respective user.

If the PLC is started with the "CODESYS Control Win SysTray PLC Control", it runs in the Windows user account "LocalSystem" and therefore the effective working directory is "C:\Windows\system32\config\systemprofile\AppData\Roaming\CODESYS\" or "C:\Windows\SysWOW64\config\systemprofile\AppData\Roaming\CODESYS\". An administrator account is required to access these folders.

6 Mitigation

Only create required user accounts on the Microsoft Windows systems on which the affected software is installed. Users who do not need to use the affected software should not have access to these systems.

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 joker63.

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=18354&token=f3e92a942c3a2f90c272a5ded7598c6a0b5f4924&download=

Change History

Version	Description	Date
1.0	Initial version	2024-05-22
2.0	Software updates available	2024-06-05