CODESYS Development System - Deserialization of Untrusted Data

CODESYS Security Advisory 2025-11

Published: 2025-12-01

Last Change: 2025-12-01

Identifiers, Type and Severity

CVE-2025-41700

CERT@VDE: VDE-2025-101

CODESYS: CDS-94858, CDS-94904

CWE-502: Deserialization of Untrusted Data

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

1 Summary

A vulnerability has been discovered in the print engine of the CODESYS development system. If a CODESYS project file or archive file was crafted in a specific way, the CODESYS development system could execute arbitrary code when a user opens these files and configures the print/printer options or prints the project or parts of it. This arbitrary code would be executed in the context of the user who was tricked into opening the project.

2 Affected Products

The following products are affected in all versions before 3.5.21.40.
• CODESYS Development System

3 Impact

The CODESYS development system deserializes potentially untrusted data and thereby executes arbitrary code when a user opens and edits a deliberately manipulated CODESYS project file with a CODESYS development system. This arbitrary code is executed in the user context and can compromise system integrity, confidentiality, and availability.

4 Remediation

Update the following products to version 3.5.21.40.
• CODESYS Development System

When existing CODESYS project files are opened with a fixed CODESYS Development system version, the option keys "PageSettings" and "PrinterSettings" are now obsolete and will be reset. As a result printer and page settings will be lost and have to be reconfigured. Only these specific parts of "Project Options -> Page Setup" are dropped by the update. The configured Header, Footer, TitlePage and Document options will be kept.

The CODESYS Development System 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 https://www.codesys.com/download/.

5 Mitigation

Open/install CODESYS archives, projects and packages from trustworthy sources only.

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.

7 Acknowledgments

Names: MengyuXia
Company: Beijing Aerospace Wanyuan Science & Technology Co, Ltd.

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 CODESYS support.

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://api-www.codesys.com/fileadmin/user_upload/CODESYS_Group/Ecosystem/Up-to-Date/Security/Security-Advisories/Advisory2025-11_CDS-94858.pdf

Change History

Version	Description	Date
1.0	Initial version	2025-12-01