CODESYS Development System V3

CODESYS Security Advisory 2023-06

Published: 2023-08-03

1   Overview

The CODESYS Development System is vulnerable to the execution of malicious binaries from the current working directory.

2   Affected Products

CODESYS Development System versions from 3.5.17.0 and before 3.5.19.20

3   Vulnerability Identifiers, Type and Severity

VDE-2023-021 [1]

CODESYS JIRA: CDS-85457, CDS-85492

CVE-2023-3662 [7]

CWE-427: Uncontrolled Search Path Element [8]

CVSS v3.1 Base Score 7.3 | High | CVSS:3.1/AV:L/AC:L/PR:L/UI:R/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. When the CODESYS Development System is installed, it is assigned the file extensions ".project", ".library" and ".projectarchive" for project files. If a project file is later double-clicked, the CODESYS Development System also searches in its folder for a specific executable file. If an attacker place such a malicious executable file there, it will be executed instead of the one contained in the CODESYS installation when the legitimate user wants to open a ".project", ".library" and ".projectarchive" file.

5   Remediation

Update the CODESYS Development System to version 3.5.19.20.

The CODESYS Development System can be downloaded and installed directly with the CODESYS Installer or be downloaded from the CODESYS Store.

Alternatively, 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

Template: templ_tecdoc_en_V3.0.docx

For more information and general recommendations for protecting machines and plants, see also the CODESYS Security Whitepaper [2].

7   Acknowledgments

This vulnerability was reported by Carlo Di Dato of Deloitte Risk Advisory Italia - Vulnerability Research Team.

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 update 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=17766&token=667d36292e99e6f6b7eb8c0b4a86d27137c31f98&download=

Change History

Version	Description	Date
1.0	Initial version	2023-07-20
2.0	Software update available	2023-08-03