CODESYS Development System V3

CODESYS Security Advisory 2023-08

Published: 2023-08-03

1 Overview

The CODESYS Development System does not limit the number of attempts to guess the password within an import dialog.

2 Affected Products

CODESYS Development System versions prior to 3.5.19.20

3 Vulnerability Identifiers, Type and Severity

VDE-2023-023 [1]

CODESYS JIRA: CDS-76333, CDS-84600

CVE-2023-3669 [7]

CWE-307: Improper Restriction of Excessive Authentication Attempts [8]

CVSS v3.1 Base Score 3.3 | Low | CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:L/I:N/A:N [9]

4 Impact

The CODESYS Development System is an IEC 61131-3 programming tool for the industrial controller and automation technology sector. Both CODESYS projects and the CODESYS Control Runtime system are protected by a user management.

The CODESYS Development System offers the option to transfer users from the CODESYS project user management into the CODESYS Control runtime user management. For this purpose, there is an import functionality in the device editor dialog for the PLC. During the import, the correct password must be entered for each imported user. However, this password query ignores the maximum number of incorrect entries defined in the project. This means that an attacker can make any number of attempts to guess the password via this import dialog.

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

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 an OEM customer.

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 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=17768&token=9d206ea9e0449cd9d3ee60d5179d2761dad2d2dd&download=

Change History

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