CODESYS Development System V2.3

CODESYS Security Advisory 2024-01

Published: 2024-05-06

1 Overview

Local attackers can cause affected CODESYS Development System V2.3 installations to crash or execute code by opening malicious project files.

The CODESYS Development System V2.3 is an IEC 61131-3 programming tool for the industrial controller and automation technology sector. It stores the program code for the controller and its configuration in project files (*.pro).

2 Affected Products

CODESYS Development System V2.3 versions prior to 2.3.9.73

3 Vulnerability Identifiers, Type and Severity

VDE-2024-024 [1]

CODESYS JIRA: LCDS-419

CVE-2023-49675, CVE-2023-49676 [7]

CWE-787: Out-of-bounds Write, CWE-416: Use After Free [8]

CVSS:3.1/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H | High | 7.8 [9]

4 Impact

The CODESYS Development System V2.3 allows corrupt project files to be opened after confirmation of a warning dialog so that legitimate users can possibly copy project fragments into a new project. This functionality does not sufficiently secure the loading of malicious project files and is therefore susceptible to the following memory corruption vulnerabilities:

CVE-2023-49675:
CWE-787: Out-of-bounds Write
CVSS:3.1/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H | 7.8 | High
An unauthenticated local attacker may trick a user to open corrupted project files to execute arbitrary code or crash the system due to an out-of-bounds write vulnerability.

CVE-2023-49676
CWE-416: Use After Free
CVSS:3.1/AV:L/AC:L/PR:N/UI:R/S:U/C:N/I:N/A:H | 5.5 | Medium
An unauthenticated local attacker may trick a user to open corrupted project files to crash the system due to use after free vulnerability.

5 Remediation

Update the CODESYS Development System V2.3 to version 2.3.9.73.

As of this version, projects recognized as corrupt can no longer be opened with the CODESYS Development System V2.3. If the CODESYS Development System V2.3 detects that the project file has been manipulated, the user will be informed, and the loading will be terminated.

Note: CODESYS V2.3 is currently in the service phase. Please consider upgrading to CODESYS V3.

Please visit the CODESYS download area for more information on how to obtain the software update [4].

6 Mitigation

CODESYS GmbH strongly recommends only opening projects from trustworthy sources!

If the following dialog appears when opening a project, please pay attention to this warning and do not try to load the affected project:
"The project file is corrupt. Would you still like to try to load the project?
Attention! CODESYS could become unstable when loading a corrupt project file."

In addition, we recommend saving projects with password encryption, which offers even more protection against tampering of the project.

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

These issues were reported by Michael Heinzl.

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=18290&token=b953e6165f59e66680a2350b4e715c63f8991424&download=

Change History

Version	Description	Date
1.0	Initial version	2024-04-25
2.0	Software update available, revision of the document	2024-05-06