Advisory 2021-03

Security update for CODESYS V3 Library Manager

Published: 28 April 2021

CONTENT

1 Affected Products

All CODESYS Development System V3 versions prior V3.5.17.0 are affected by this vulnerability. This applies to both the 32-bit and 64-bit variants.

2 Vulnerability overview

2.1 Type

CWE-345: Insufficient Verification of Data Authenticity [7]

2.2 Management Summary

The CODESYS Development System displays or executes malicious documents or files embedded in libraries without first checking their validity.

2.3 References

CVE: CVE-2021-29239 [6]

CODESYS JIRA: CDS-71069

2.4 Severity Rating

CODESYS GmbH has rated this vulnerability as high.

The CVSS v3.0 base score of 7.8 has been assigned. The CVSS vector string is (CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H). [8]

3 Vulnerability details

3.1 Detailed Description

The CODESYS Development System is an IEC 61131-3 programming tool for the industrial controller and automation technology sector. The source code of CODESYS projects or parts of it can be packaged into compiled libraries to pass this code on or use it in other projects. The CODESYS library format allows also adding further files to the libraries. This is often used for documentation or additional visualization files. The CODESYS Development System displays or executes malicious documents or files embedded in libraries without first checking their validity.

3.2 Exploitability

This vulnerability could be exploited by or with the help of local users.

3.3 Difficulty

An attacker with low skills would be able to exploit this vulnerability.

3.4 Existence of exploit

No known public exploits specifically target this vulnerability.

4 Available software updates

CODESYS GmbH has released version V3.5.17.0 to solve the noted vulnerability issue for all affected products.

Please visit the CODESYS update area for more information on how to obtain the software update [3].

Since CODESYS V3.5.17.0, documents or files embedded in a library are only displayed or executed, if the library was correctly signed with a valid certificate. Therefore, we have updated all CODESYS libraries to version V3.5.17.0 and signed them to make them trustworthy.

Template: templ_tecdoc_en_V3.0.docx

CODESYS GmbH also encourages all library vendors to sign their libraries so that they are displayed and treated as trusted.

5   Mitigation

CODESYS GmbH recommends using the available software update to fix the vulnerability.

CODESYS GmbH has currently found no workaround for this vulnerability. Therefore, you should only install and use CODESYS libraries from trustworthy sources, in case the software update is not applied.

As part of a security strategy, CODESYS GmbH recommends the following general defense measures to reduce the risk of exploits:
• 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
• Use VPN (Virtual Private Networks) tunnels if remote access is required
• Activate and apply user management and password features
• Use encrypted communication links
• Limit the access to both development and control system by physical means, operating system features, etc.
• 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 [1].

6   Acknowledgments

CODESYS GmbH thanks those in the security community, who help us to improve our products and to protect customers and users through coordinated vulnerability disclosure.

We thank an OEM customer for reporting this vulnerability following coordinated disclosure.

7   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 [5].

8   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.

Template: templ_tecdoc_en_V3.0.docx

Bibliography

[1] CODESYS GmbH: CODESYS Security Whitepaper

[2] CODESYS GmbH: Coordinated Disclosure Policy

[3] CODESYS GmbH update area: https://www.codesys.com/download

[4] CODESYS GmbH security information page: https://www.codesys.com/security

[5] CODESYS GmbH support contact site: https://www.codesys.com/support

[6] Common Vulnerabilities and Exposures (CVE): https://cve.mitre.org

[7] Common Weakness Enumeration (CWE): https://cwe.mitre.org

[8] CVSS Calculator: https://www.first.org/cvss/calculator/3.0

[9] ICS-CERT: https://ics-cert.us-cert.gov

The latest version of this document can be found here:

https://customers.codesys.com/index.php?eID=dumpFile&t=f&f=14639&token=fa836f8bd4a2184aa9323a639ca9f2aaf1538412&download=

Change History

Version	Description	Date
1.0	First version	29.03.2021
2.0	Software update available	28.04.2021