Advisory 2022-15

Security update for CODESYS V3 boot application encryption

Published: 14 December 2022

Version: 2.0
Template: templ_tecdoc_en_V3.0.docx
File name: Advisory2022-15_CDS-82335.docx

CONTENT

Page

1 Affected Products 3

2 Vulnerability overview 3

2.1 Type 3
2.2 Management Summary 3
2.3 References 3
2.4 Severity Rating 3

3 Vulnerability details 3

3.1 Detailed Description 3
3.2 Exploitability 3
3.3 Difficulty 3
3.4 Existence of exploit 3

4 Available software updates 4

5 Mitigation 4

6 Acknowledgments 4

7 Further Information 4

8 Disclaimer 5

Bibliography 5

Change History 5

1 Affected Products

All CODESYS Development System V3 versions prior to V3.5.18.40 are affected by this vulnerability. This applies to both the 32-bit and 64-bit variants.

2 Vulnerability overview

2.1 Type

CWE-326: Inadequate Encryption Strength [7]

2.2 Management Summary

The implementation of the CODESYS boot application encryption based on the CODESYS Runtime Key or Wibu-Systems CodeMeter dongle/ flash card uses weak cryptography.

2.3 References

CVE: CVE-2022-4048 [6]

CODESYS JIRA: CDS-82335, CDS-82344

2.4 Severity Rating

CODESYS GmbH has rated this vulnerability as high.

The CVSS v3.1 base score of 7.7 has been assigned. The CVSS vector string is (CVSS:3.1/AV:L/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:N). [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. It contains an integrated compiler for generating code for execution on the CODESYS Control runtime systems.

For over 10 years, starting with version V3.5, the CODESYS Development System has supported optional encryption through a dongle using Wibu-System's CodeMeter technology. This hardware dongle can either be a USB stick (CODESYS Runtime Key) or a special pre-programmed flash card offered by Wibu-Systems.

The implementation of the CODESYS boot application encryption based on the CODESYS Runtime Key or the Wibu-System CodeMeter dongle/ flash card uses weak cryptography. The vulnerable encrypted boot application is downloaded to and executed by the CODESYS Control runtime systems. This allows an attacker to decrypt the boot application and access and manipulate the compiled code.

In version V3.5.10.0, CODESYS GmbH introduced an alternative protection of the downloaded code by signing and/or encrypting it using X.509 certificates. This is not affected by the vulnerability described above. All other use cases of the CODESYS Runtime Key or the Wibu-System CodeMeter dongle/ flash card are not affected by this vulnerability either.

3.2 Exploitability

The CODESYS boot application file could be exploited.

3.3 Difficulty

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

3.4 Existence of exploit

No known public exploits specifically target this vulnerability in CODESYS products.

4 Available software updates

CODESYS GmbH has released version V3.5.18.40, which solves the identified security vulnerabilities for the affected product.

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 [3].

To make the fix effective for existing CODESYS projects, you must change the application properties for security from "Encryption with license management" to "Encryption with certificates", configure the certificates to be used for encryption, and perform a new download to the PLC. This is possible with all CODESYS Development System versions V3.5.10.0 or newer, as these already support the alternative protection of the downloaded code by signing and/or encrypting with X.509 certificates.

CODESYS Development System version V3.5.18.40 warns each time the application is downloaded to the PLC if dongle encryption is used and suggests protecting the application with certificates. For new and existing CODESYS projects, a similar warning is displayed in the application's properties dialog if the user selects the vulnerable encryption based on the CODESYS Runtime Key or the Wibu-System CodeMeter dongle/ flash card. For compatibility reasons, we could not completely remove this type of application encryption.

5 Mitigation

If the affected CODESYS boot application encryption based on the CODESYS Runtime Key or Wibu system CodeMeter dongle/ flash card is used, then CODESYS GmbH recommends using a CODESYS Development System and a CODESYS Control runtime system of version V3.5.10.0 or higher and protecting the downloaded code by signing and/or encrypting with X.509 certificates.

To make the fix effective for existing CODESYS projects, you must change the application properties for security from "Encryption with license management" to "Encryption with certificates", configure the certificates to be used for encryption, and perform a new download to the PLC. The "Encryption with certificates" security setting is also recommended for new CODESYS projects.

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

The vulnerability was discovered by Abdelrahman Hassanien and Jos Wetzels, Forescout Technologies.

CODESYS GmbH thanks for reporting following coordinated disclosure. This helps us to improve our products and to protect customers and users.

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.

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/3.1
[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=17350&token=2cee62285d3ec76d6a78dfa9b9e81e66f6136a2a&download=

Change History

Version	Description	Date
1.0	First version	23.11.2022
2.0	Software update available	14.12.2022