Advisory 2022-11

Security update for CODESYS Control V2

Published: 23 June 2022

Version: 2.0
Template: templ_tecdoc_en_V3.0.docx
File name: Advisory2022-11_LCDS-363.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 4
3.3 Difficulty 4
3.4 Existence of exploit 4

4 Available software updates 4

5 Mitigation 5

6 Acknowledgments 5

7 Further Information 5

8 Disclaimer 5

Bibliography 6

Change History 6

1 Affected Products

The following CODESYS V2 runtime systems are affected, regardless of the CPU type or operating system:

- CODESYS Runtime Toolkit 32 bit full prior version V2.4.7.57
- CODESYS PLCWinNT prior version V2.4.7.57

2 Vulnerability overview

2.1 Type

Several, see detailed description.

2.2 Management Summary

CODESYS Control V2 runtime systems are affected by several security vulnerabilities in the communication server for the CODESYS protocol. These can be exploited by authenticated attackers.

2.3 References

CVE: CVE-2022-1965, CVE-2022-32136, CVE-2022-32137, CVE-2022-32138, CVE-2022-32139, CVE-2022-32140, CVE-2022-32141, CVE-2022-32142, CVE-2022-32143 [6]

CODESYS JIRA: LCDS-363, LCDS-368

2.4 Severity Rating

CODESYS GmbH has rated this vulnerability as high.

The CVSS v3.1 base score of 8.8 has been assigned. The CVSS vector string is (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H). [8]

3 Vulnerability details

3.1 Detailed Description

The CODESYS Control runtime system enables embedded or PC-based devices to be a programmable industrial controller. It provides a communication server for the communication with clients like the CODESYS Development System.

Since the CODESYS Control V2 runtime system only processes service requests after authentication, all the following security vulnerabilities can only be exploited if the attacker has previously successfully authenticated himself on the controller or if no level 1 online password is configured on the controller.

CVE-2022-1965: CWE-755: Improper Handling of Exceptional Conditions
CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H
An invalid crafted request is not properly processed by the error handling of the affected CODESYS products. As a result, the file referenced by the malicious request could be deleted if it exists on the controller.

CVE-2022-32136: CWE-824: Access of Uninitialized Pointer
CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H
A crafted request may cause an internal read access to an uninitialized pointer in the affected CODESYS products, resulting in a denial-of-service condition.

CVE-2022-32137: CWE-122: Heap-based Buffer Overflow
CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H
A crafted request may cause a heap-based buffer overflow in the affected CODESYS products, resulting in a denial-of-service condition or memory overwrite.

CVE-2022-32138: CWE-194: Unexpected Sign Extension
CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H
A crafted request with may cause an unexpected sign extension in the affected CODESYS products, resulting in

a denial-of-service condition or memory overwrite.

CVE-2022-32139: CWE-125: Out-of-bounds Read
CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H
A crafted request may cause an internal out-of-bounds read in the affected CODESYS products, resulting in a denial-of-service condition.

CVE-2022-32140: CWE-130: Improper Handling of Length Parameter Inconsistency
CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H
A crafted request may contain an incorrect data length for the associated structured data of the request. Since the affected CODESYS products do not handle the length correctly, this can lead to an internal buffer over-read causing a denial-of-service condition.

CVE-2022-32141: CWE-126: Buffer Over-read
CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H
A crafted request with invalid offsets may cause an internal buffer over-read in the affected CODESYS products, resulting in a denial-of-service condition.

CVE-2022-32142: CWE-823: Use of Out-of-range Pointer Offset
CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:H/A:H
A crafted request with invalid offsets may cause an internal out-of-bounds read or write access in the affected CODESYS products, resulting in a denial-of-service condition or local memory overwrite.

CVE-2022-32143: CWE-552: Files or Directories Accessible to External Parties
CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H
The CODESYS V2 file download and upload function also allows read and potentially write access to internal files in the working directory, e.g. firmware files of the PLC, since no filtering is performed.

3.2 Exploitability

These vulnerabilities could be exploited remotely.

3.3 Difficulty

An attacker with low skills would be able to exploit these vulnerabilities.

3.4 Existence of exploit

No known public exploits specifically target these vulnerabilities.

4 Available software updates

CODESYS GmbH has released the following product versions to solve the noted vulnerability issues for the affected CODESYS products:

• CODESYS Runtime Toolkit 32 bit full version V2.4.7.57
• CODESYS PLCWinNT version V2.4.7.57. This is also part of the CODESYS Development System setup version V2.3.9.69.

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

Additional information for device manufacturers

Relates to CVE-2022-32143: CWE-552: Files or Directories Accessible to External Parties:

The newly introduced process hook PH_DENY_FILE allows protecting additional device-specific files from access by online services. For details see the description of PH_DENY_FILE in RtsApi.h.

5 Mitigation

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

To exploit these vulnerabilities, a successful login to the affected product is required. A configured PLC password for password level 1 therefore protects against the exploitation of these vulnerabilities even in case the software update could not be applied.

CODESYS GmbH strongly recommends setting a strong PLC password. This not only prevents malicious requests from being executed or virulent code from being downloaded, but also suppresses starting, stopping, debugging or other actions on a known working application that could potentially disrupt a machine or system.

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

These issues were reported by Gao Jian of NSFOCUS.

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=17139&token=ec67d15a433b61c77154166c20c78036540cacb0&download=

Change History

Version	Description	Date
1.0	First version	09.06.2022
2.0	Software update available	23.06.2022