Advisory 2022-12

Security update for CODESYS V2 password transport

Published: 14 December 2022

Version: 4.0
Template: templ_tecdoc_en_V3.0.docx
File name: Advisory2022-12_LCDS-364.docx

CONTENT

1 Affected Products

The following CODESYS V2 products are affected, regardless of the CPU type or operating system:
• CODESYS Development System prior version V2.3.9.69
• CODESYS Gateway Client prior version V2.3.9.38
• CODESYS Gateway Server prior version V2.3.9.38
• CODESYS Web server prior version V1.1.9.23
• CODESYS SP Realtime NT prior version V2.3.7.30
• CODESYS PLCWinNT prior version V2.4.7.57
• CODESYS Runtime Toolkit 32 bit full prior version V2.4.7.57

In addition, the following CODESYS V3 products can communicate as a client with CODESYS V2 runtime systems and are insofar also affected in all versions prior to V3.5.18.40:
• CODESYS Development System
• CODESYS Gateway
• CODESYS Edge Gateway for Windows
• CODESYS HMI (SL)
• CODESYS OPC DA Server SL
• CODESYS PLCHandler

2 Vulnerability overview

2.1 Type

CWE-523: Unprotected Transport of Credentials, CWE-1188: Insecure Default Initialization of Resource [7]

2.2 Management Summary

The CODESYS V2 communication protocol transmits passwords unprotected. Also, password protection is not activated by default for the CODESYS Control runtime system V2.

2.3 References

CVE: CVE-2022-31805, CVE-2022-31806 [6]

CODESYS JIRA: LCDS-364, LCDS-367, LCDS-377, LCDS-378, LCDS-379, LCDS-380, LCDS-382, LCDS-383, LCDS-384, CDS-81289, CDS-81314

2.4 Severity Rating

CODESYS GmbH has rated this vulnerability as critical.

The CVSS v3.1 base score of 9.8 has been assigned. The CVSS vector string is (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H). [8]

3 Vulnerability details

3.1 Detailed Description

The CODESYS communication protocol allows clients like the CODESYS Development System or the CODESYS PLCHandler to communicate directly or via the CODESYS Gateway to CODESYS Control runtime systems. The CODESYS Control runtime systems enables embedded or PC-based devices to be a programmable industrial controller. To protect against unauthorized access, the communication servers of products such as the CODESYS Control runtime system can be protected with a password. This feature has the following vulnerabilities:

CVE-2022-31805: CWE-523: Unprotected Transport of Credentials
The passwords between the communication clients and servers among the affected products are transmitted unprotected. This allows attackers to guess passwords if they are able to sniff the communication.

CVE-2022-31806: CWE-1188: Insecure Default Initialization of Resource
Password protection is not enabled by default and there is no information or prompt to enable password protection at login in case no password is set at the controller.

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 Development System version V2.3.9.69
- CODESYS Gateway Client version V2.3.9.38
- CODESYS Gateway Server version V2.3.9.38
- CODESYS Web server version V1.1.9.23
- CODESYS SP Realtime NT version V2.3.7.30
- CODESYS PLCWinNT version V2.4.7.57
- CODESYS Runtime Toolkit 32 bit full version V2.4.7.57

For the below listed CODESYS V3 products, CODESYS GmbH has released version V3.5.18.40 to solve the password transport vulnerability CVE-2022-31805 on client side:

- CODESYS Development System
- CODESYS Gateway
- CODESYS Edge Gateway for Windows
- CODESYS HMI (SL)
- CODESYS OPC DA Server SL
- CODESYS PLCHandler

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

To eliminate the password transport vulnerability CVE-2022-31805, an update of all products involved in the communication is required.

As CODESYS V2 is a legacy product, we could not enforce a PLC password by default in a compatible way to solve CVE-2022-31806. Instead, the CODESYS development system reminds the PLC programmer at login to activate PLC password protection if a password has not yet been set on the PLC. Acting on this hint secures both current and old PLC runtime versions.

5 Mitigation

CODESYS GmbH recommends using the available software update to fix the vulnerabilities and setting a strong PLC password.

Currently, CODESYS GmbH has not identified any specific workarounds for these vulnerabilities, 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

CVE-2022-31805: This issue was reported by Gao Jian of NSFOCUS.

CVE-2022-31806: This issue was reported by Chen Jie 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=17140&token=6aa2c5c4a8b83b8b09936fefed5b0b11f9d2cc6c&download=

Change History

Version	Description	Date
1.0	First version	09.06.2022
2.0	Software update available, CWE adjusted	23.06.2022
3.0	Release of CODESYS V3 products (communication clients) postponed, CODESYS V3 JIRA references added	06.10.2022
4.0	Software update available	14.12.2022