Advisory 2022-10

Security update for CODESYS OPC DA Server V3

Published: 06 October 2022

Version: 4.0
Template: templ_tecdoc_en_V3.0.docx
File name: Advisory2022-10_CDS-37625.docx

CONTENT

1 Affected Products

All versions prior V3.5.18.20 of the following CODESYS V3 product are affected by this vulnerability:
• CODESYS OPC DA Server SL

2 Vulnerability overview

2.1 Type

CWE-256: Plaintext Storage of a Password [7]

2.2 Management Summary

The CODESYS OPC DA Server stores PLC passwords as plain text in its configuration file so that it is visible to all authorized Microsoft Windows users of the system.

2.3 References

CVE: CVE-2022-1794 [6]

CODESYS JIRA: CDS-37625, CDS-81306

2.4 Severity Rating

CODESYS GmbH has rated this vulnerability as medium.

The CVSS v3.1 base score of 5.5 has been assigned. The CVSS vector string is (CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N). [8]

3 Vulnerability details

3.1 Detailed Description

The CODESYS OPC DA Server is a program that runs on Microsoft Windows systems and enables access to the data of an automation process in accordance with the OPC (Open Platform Communications) standard interface. The main task of the CODESYS OPC DA Server is the exchange of data (read / write) with the controller, e.g. for visualizations or for process data acquisition programs. In order to access the data, the CODESYS OPC DA Server must connect to CODESYS V2.3 or CODESYS V3 based controllers via the CODESYS protocol and authenticate to them.

The credentials for the CODESYS OPC DA Server account on the PLC are stored in plain text as part of the connection parameters in the configuration file. This allows other authorized Microsoft Windows users of the system running the CODESYS OPC DA Server to read the configured passwords.

3.2 Exploitability

This vulnerability could be exploited by local users, which have access to the configuration file.

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 in CODESYS products.

4 Available software updates

CODESYS GmbH has released version V3.5.18.20, which solves the identified security vulnerabilities for the affected product:
• CODESYS OPC DA Server SL

The latest version can be downloaded from the CODESYS Store. Alternatively, you will find further information on obtaining the software update in the CODESYS Update area [3].

After updating the CODESYS OPC DA Server via the setup, the new CODESYS OPC DA Server removes plain text passwords from the configuration file at startup and stores them in the Microsoft Windows Credential Manager instead.

Further password specific information can be found in the chapter “Passwords in OPCConfig” of the CODESYS_OPC_Server_V3_User_Guide.pdf, which is available in the installation directory of the CODESYS OPC DA Server. Especially the use of the CODESYS OPCConfig tool, the deployment of CODESYS OPC DA Server configuration files to multiple PCs and other compatibility aspects are described there in detail.

5 Mitigation

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

Currently, CODESYS GmbH has not identified any specific workarounds for this vulnerability, in case the software update is not applied.

CODESYS GmbH strongly recommends creating and using a separate user in the user management of the controller for OPC DA communication. This user shall have only the minimum access rights to the required symbols of the controller and, for example, no permission to program the controller.

Furthermore, saving and transporting configuration files for the CODESYS OPC DA server requires the utmost care and, if necessary, further access protection measures if credentials are stored in such files.

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 found internally by the CODESYS team.

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=17129&token=1c1485c4a700c04f2069699f5be7558d276ca117&download=

Change History

Version	Description	Date
1.0	First version	19.05.2022
2.0	CVE added, CVSS adapted, Software update available	30.05.2022
3.0	Software versions adapted, as V3.5.18.10 was withdrawn	03.06.2022
4.0	CVSS adapted	06.10.2022