Advisory 2022-14

Security update for CODESYS V3 Visualization

Published: 06 October 2022

Version: 3.0
Template: templ_tecdoc_en_V3.0.docx
File name: Advisory2022-14_VIS-1504.docx

CONTENT

1 Affected Products

All CODESYS Visualization versions prior to V4.2.0.0 provide a weak login dialog and inject it into the generated code, which is downloaded to and executed by the HMI or PLC.

CODESYS Visualization versions prior to V3.5.17.0 were provided as integrated plugins of the CODESYS Development System. This means that all CODESYS Development System versions before V3.5.17.0 generate a vulnerable login-dialog.

As of CODESYS Development System V3.5.17.0, CODESYS Visualization is provided as an optional Add-on and can be updated separately. CODESYS Visualization V4.0.0.0 was the first version to be made available as an optional Add-on and delivered together with CODESYS Development System V3.5.17.0. Thus, the Visualization Add-on versions from V4.0.0.0 and before V4.2.0.0 generate a vulnerable login-dialog.

2 Vulnerability overview

2.1 Type

CWE-204: Observable Response Discrepancy [7]

2.2 Management Summary

Login-dialog of the CODESYS Visualization discloses the information whether a user is existing or not.

2.3 References

CVE: CVE-2022-1989 [6]

CODESYS JIRA: VIS-1504

2.4 Severity Rating

CODESYS GmbH has rated this vulnerability as medium.

The CVSS v3.1 base score of 5.3 has been assigned. The CVSS vector string is (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N). [8]

3 Vulnerability details

3.1 Detailed Description

The CODESYS Visualization is an integrated visualization editor for the CODESYS Development System. To secure the visualization screens or elements, CODESYS Visualization has an integrated role-based user management. To authenticate at the user management, the CODESYS visualization provides a login-dialog. The login-dialog is downloaded to the HMI or PLC as part of the created visualizations and displayed by the CODESYS HMI, CODESYS TargetVisu or CODESYS WebVisu.

This dialog returns different feedback for invalid user and password, so that an attacker can determine whether a user exists or not.

3.2 Exploitability

This vulnerability could be exploited remotely.

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 V4.2.0.0 of CODESYS Visualization to solve the noted vulnerability issue. CODESYS Visualization V4.2.0.0 can be downloaded and installed directly with the CODESYS Installer. This requires a CODESYS Development System version of V3.5.17.0 or newer.

Older CODESYS Development System versions must be updated first.

To make the fix effective for existing CODESYS projects, you must additionally recompile the CODESYS application containing the dialog and perform a download to the HMI or PLC.

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.

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

This vulnerability was reported by an OEM customer.

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=17142&token=a3696ab41fef800d2eaee8043d40d5fbe94277fd&download=

Change History

Version	Description	Date
1.0	First version	03.06.2022
2.0	CVE added	03.06.2022
3.0	CVSS adapted	06.10.2022