Advisory 2020-04

Security update for CODESYS V3 Visualization

Published: 06 May 2020

Version: 2.0
Template: templ_tecdoc_en_V3.0.docx
File name: Advisory2020-04_CDS-66210.docx

CONTENT

1 Affected Products

The CODESYS Development System's compiler generates code for the integrated CODESYS visualization, which is then executed on the CODESYS Control runtime systems.

All CODESYS Development System V3 versions prior V3.5.16.0 imply this vulnerability to the generated code. This is true for both the 32-bit and 64-bit variants.

As a part of the fix was done in the CmpWebServerHandlerV3, all the following CODESYS runtime products are additional affected in all versions prior V3.5.16.0, regardless of the CPU type or operating system:

- CODESYS Control for BeagleBone
- CODESYS Control for emPC-A/iMX6
- CODESYS Control for IOT2000
- CODESYS Control for Linux
- CODESYS Control for PLCnext
- CODESYS Control for PFC100
- CODESYS Control for PFC200
- CODESYS Control for Raspberry Pi
- CODESYS Control RTE V3
- CODESYS Control RTE V3 (for Beckhoff CX)
- CODESYS Control Win V3 (also part of the CODESYS Development System setup)
- CODESYS HMI V3
- CODESYS Control V3 Runtime System Toolkit

2 Vulnerability overview

2.1 Type

Improper Privilege Management

2.2 Management Summary

Certain configurations of the CODESYS visualization are susceptible to a privilege escalation attack allowing access to visualization screens that are intended only for specific operators.

2.3 References

CVE: CVE-2020-12068 [6]

CODESYS JIRA: CDS-66210

2.4 Severity Rating

3S-Smart Software Solutions GmbH has rated this vulnerability as medium.

The CVSS v3.0 base score of 6.5 has been assigned. The CVSS vector string is (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:N). [7]

3 Vulnerability details

3.1 Detailed Description

The CODESYS visualization provides several display variants that can be used for displaying visualization screens. Using the User management feature of the visualization, it is possible to restrict access to parts of the visualization for certain operators.

The CODESYS WebVisu and the CODESYS Remote TargetVisu are susceptible to a privilege escalation allowing access to visualization screens that are intended solely for specific operators. This attack is only possible under one of the following constellations:

• The navigation inside the downloaded visualization is done by switching the entire visualization screens and only the elements for the navigation are protected by the User management.

• The downloaded visualization contains visualization screens that cannot be reached by navigation.

As the vulnerability affects the visualization feature itself, therefore the CODESYS Control runtime products are only affected, if the visualization feature is used.

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.

4 Available software updates

3S-Smart Software Solutions GmbH has released version V3.5.16.0 to solve the noted vulnerability issue for all affected CODESYS products.

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

To fix the vulnerability an update of the CODESYS Development system is needed. If the CODESYS WebVisu is used, an update of the involved CODESYS Control runtime system running the Webserver is necessary too. In the CODESYS Development system, the fix is bound to the visualization profile. Starting with visualization profile V3.5.16.0, only the configured start visualizations (in the visualization clients below the Visualization Manager) are allowed to be accessed. Therefore the effective visualization profiles in the CODESYS project must be set to a version >= V3.5.16.0 to make the fix effective.

The previous behavior can be restored by setting the compiler define VISU_NO_STARTVISU_CHECK. However, this is recommended only for compatibility. Instead of setting this compiler define, you should add additional visualization client objects to have several start visualizations.

5 Mitigation

3S-Smart Software Solutions GmbH recommends using the available software update to fix the vulnerabilities.

3S-Smart Software Solutions GmbH has identified the following workarounds for this vulnerability, in case the software update is not applied:

• Use frames for navigation instead of switching the entire visualization screen.

• Use the protection of the User management in the CODESYS visualization not only for the navigation elements but also for all elements that should be restricted to certain operators only.

• Only include visualization screens in the application that are intended for being accessed by operators of the CODESYS WebVisu and the CODESYS Remote TargetVisu.

As part of a security strategy, 3S-Smart Software Solutions 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

• 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

3S-Smart Software Solutions GmbH thanks those in the security community, who help us to improve our products and to protect customers and users through coordinated vulnerability disclosure.

This vulnerability was reported internally by the CODESYS Security Team.

7 Further Information

For additional information regarding the CODESYS products, especially the above-mentioned versions, or about the described vulnerability please contact the 3S-Smart Software Solutions support team [5].

8 Disclaimer

Bibliography

[1] 3S-Smart Software Solutions GmbH: CODESYS Security Whitepaper
[2] 3S-Smart Software Solutions GmbH: Coordinated Disclosure Policy
[3] 3S-Smart Software Solutions GmbH CODESYS update area: https://www.codesys.com/download
[4] 3S-Smart Software Solutions GmbH security information page: https://www.codesys.com/security
[5] 3S-Smart Software Solutions GmbH support contact site: https://www.codesys.com/support
[6] Common Vulnerabilities and Exposures (CVE): https://cve.mitre.org
[7] CVSS Calculator: https://www.first.org/cvss/calculator/3.0
[8] 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=13136&token=c267875c01ea70bc9613bc39c684eedc17f55420&download=

Change History

Version	Description	Date
1.0	First version	24.04.2020
2.0	Software update available	06.05.2020