Advisory 2021-01

Security update for various CODESYS V3 products using the CODESYS communication protocol

Published: 18 May 2021

Version: 3.0
Template: templ_tecdoc_en_V3.0.docx
File name: Advisory2021-01_CDS-67954.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**	**4**
3.1	Detailed Description	4
3.2	Exploitability	4
3.3	Difficulty	4
3.4	Existence of exploit	4
4	**Available software updates**	**4**
5	**Mitigation**	**5**
6	**Acknowledgments**	**6**
7	**Further Information**	**6**
8	**Disclaimer**	**6**
Bibliography		**7**
Change History		**7**

1 Affected Products

All variants of the following CODESYS V3 products in all versions prior V3.5.17.0 containing the CmpChannelServer, CmpChannelServerEmbedded, CmpRouter or CmpRouterEmbedded component are affected, regardless of the CPU type or operating system:

- CODESYS Control RTE V3
- CODESYS Control RTE V3 (for Beckhoff CX)
- CODESYS Control Win V3
- CODESYS Control V3 Runtime System Toolkit
- CODESYS V3 Embedded Target Visu Toolkit
- CODESYS V3 Remote Target Visu Toolkit
- CODESYS V3 Safety SIL2
- CODESYS Edge Gateway for Windows
- CODESYS Gateway V3
- CODESYS HMI V3
- CODESYS OPC Server V3
- CODESYS PLCHandler SDK
- CODESYS V3 Simulation Runtime (part of the CODESYS Development System)

In addition, the following products based on the CODESYS Control V3 Runtime System Toolkit are affected in all versions prior to V4.1.0.0:

- CODESYS Control for BeagleBone SL
- CODESYS Control for emPC-A/iMX6 SL
- CODESYS Control for IOT2000 SL
- CODESYS Control for Linux SL
- CODESYS Control for Linux ARM SL
- CODESYS Control for PLCnext SL
- CODESYS Control for PFC100 SL
- CODESYS Control for PFC200 SL
- CODESYS Control for Raspberry Pi SL
- CODESYS Control for WAGO Touch Panels 600 SL
- CODESYS Edge Gateway for Linux

2 Vulnerability overview

2.1 Type

CWE-20: Improper Input Validation [7]

2.2 Management Summary

Attackers can send crafted communication packets to change the routers addressing scheme and may re-route, add, remove or change low level communication packages.

2.3 References

CVE: CVE-2021-29242 [6]

CODESYS JIRA: CDS-67954, CDS-29812, CDS-63454, CDS-70293, CDS-74896

2.4 Severity Rating

CODESYS GmbH has rated this vulnerability as high.

The CVSS v3.0 base score of 8.3 has been assigned. The CVSS vector string is (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:C/C:L/I:L/A:L). [8]

3 Vulnerability details

3.1 Detailed Description

CODESYS products support a routing protocol for the communication between clients (CODESYS Development System, CODESYS HMI, CODESYS OPC Server, PLCHandler, Remote Target Visu, etc.) and the CODESYS Control runtime system. Attackers can send crafted communication packets to change the routers addressing scheme and may re-route, add, remove or change low level communication packages.

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

CODESYS GmbH has released version V3.5.17.0 to solve the noted vulnerability issue for the following products:

- CODESYS Control RTE V3
- CODESYS Control RTE V3 (for Beckhoff CX)
- CODESYS Control Win V3
- CODESYS Control V3 Runtime System Toolkit
- CODESYS V3 Embedded Target Visu Toolkit
- CODESYS V3 Remote Target Visu Toolkit
- CODESYS V3 Safety SIL2
- CODESYS Edge Gateway for Windows
- CODESYS Gateway V3
- CODESYS HMI V3
- CODESYS OPC Server V3
- CODESYS PLCHandler SDK
- CODESYS V3 Simulation Runtime (part of the CODESYS Development System)

For the below listed products, CODESYS GmbH has released version V4.1.0.0 based on the CODESYS Control V3 Runtime System Toolkit V3.5.17.0:

- CODESYS Control for BeagleBone SL
- CODESYS Control for emPC-A/iMX6 SL
- CODESYS Control for IOT2000 SL
- CODESYS Control for Linux SL
- CODESYS Control for Linux ARM SL
- CODESYS Control for PLCnext SL
- CODESYS Control for PFC100 SL
- CODESYS Control for PFC200 SL
- CODESYS Control for Raspberry Pi SL
- CODESYS Control for WAGO Touch Panels 600 SL
- CODESYS Edge Gateway for Linux

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

In addition to fixing the vulnerability, the router has been hardened overall. In this context, the verification of received packets has been made more stringent and previously unused routing features have been deactivated.

At the same time, the need for manual adjustments to the router configuration has been significantly reduced by optimizing the default values. As a result, the update of the affected products, in particular the CODESYS Gateway, may result in new CODESYS addresses for the controllers in the network.

If CODESYS programmable controllers are addressed by clients such as CODESYS HMI, CODESYS OPC Server, PLCHandler, etc. via CODESYS addresses, their configuration may have to be adapted accordingly. If, on the other hand, the connection to the controller was configured by node name, hostname or IP address, which is recommended in general, then the clients will find the corresponding controller again automatically.

Furthermore, if you have manually adapted the router configuration of the CODESYS Gateway or other CODESYS based products in the past, then some details may be helpful:

As part of these changes, all subnets were removed from the CODESYS gateway configuration, as they were no longer necessary since the introduction of the parallel routing feature several years ago. As a result, the default value for the max. number of router instances "MaxRouters" has been increased from 7 to 16. This enables the CmpRouter in nearly all cases to assign the block driver instances to the router instances without the need of any configuration. As rule, you should change the configuration of CmpRouter only, if this is really needed and keep modifications as small as possible, so that the router can adapt optimally dynamically to the actual situation.

Already in the past, subnets were used almost solely for local connections, for example for the CmpBlkDrvShm (shared memory). In order to prevent misconfigurations, sending and receiving of address notifications and address requests of the CODESYS protocol has now been disabled for all networking-capable CODESYS block drivers. Specifically, this affects CmpBlkDrvCanClient, CmpBlkDrvCanServer, CmpBlkDrvTcp and CmpBlkDrvUdp. This means that they can no longer be used as subnets of the router unless an "AddressUpdateInterval" other than 0 is configured explicitly.

In summary, your previous router configuration will continue to work unless you have configured one of the network-capable block drivers as a subnet. Nevertheless, the update to version V3.5.17.0 is a good time to check whether the router configuration used so far can be returned to the default configuration or at least simplified.

Device manufacturers may have three additional points to consider for certain setups:

• PLCs containing an SIL2 or SIL3 runtime: If the address of this runtime is calculated from the address of the main PLC by adding an address postfix, which is specified in the device description by one of the settings "compound_plc_address_postfix" or "set_active_path_for_child", then this postfix may have changed. CODESYS GmbH recommends adapting the value of these device description settings e.g. from "8001" to "0001", and to keep the device description consistent to the runtime version. As an alternative the setting "MaxRouters=7" can be set in the section [CmpRouter] of the main PLC to restore the old default value for the address postfix.

• Device manufacturer specific block driver implementations: If your block driver was previously used as subnet in the router configuration of the CODESYS Gateway or other devices, please check if the block driver generates unique local addresses for all connected peers. In this case, all communication peers connected by this driver can also use it as main net. If not, you have to adapt the block driver accordingly or to continue to use it within a subnet configuration.

• The function RouterRegisterProtocolHandler() was completely removed, as it was marked as obsolete since V3.5.10.0. Please use ServerRegisterProtocolHandler() instead (services must be adapted).

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

CODESYS 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 found by Alexander Nochvay from Kaspersky Lab ICS CERT and 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 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/3.0
[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=14640&token=623b6fceb0579ef0f7505e29beefa5b3f8ac7873&download=

Change History

Version	Description	Date
1.0	First version	29.03.2021
2.0	Software update available	28.04.2021
3.0	Further software update available	18.05.2021