Advisory 2020-02

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

Published: 22 July 2020

Version: 6.0
Template: templ_tecdoc_en_V3.0.docx
File name: Advisory2020-02_CDS-69663.docx

CONTENT

1 Affected Products

All variants of the following CODESYS V3 products in all versions prior V3.5.16.10 containing the CmpRouter or CmpRouterEmbedded component are affected, 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 Linux ARM
• CODESYS Control for PLCnext
• CODESYS Control for PFC100
• CODESYS Control for PFC200
• CODESYS Control for Raspberry Pi
• CODESYS Control for WAGO Touch Panels 600
• CODESYS Control RTE V3
• CODESYS Control RTE V3 (for Beckhoff CX)
• CODESYS Control Win V3 (also part of the CODESYS Development System setup)
• 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 V3
• CODESYS Gateway V3
• CODESYS HMI V3
• CODESYS OPC Server V3
• CODESYS PLCHandler SDK
• CODESYS V3 Simulation Runtime (part of the CODESYS Development System)

2 Vulnerability overview

2.1 Type

CWE-125: Out-of-bounds Read [7]

2.2 Management Summary

Crafted communication packets can trigger an out-of-bounds memory buffer access in the communication stack, which may result in a denial-of-service condition.

2.3 References

CVE: CVE-2019-5105 [6]

CODESYS JIRA: CDS-69663, CDS-69665, CDS-69698, CDS-69876, CDS-71310, CDS-71393

2.4 Severity Rating

CODESYS GmbH has rated this vulnerability as high.

The CVSS v3.0 base score of 7.5 has been assigned. The CVSS vector string is (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H). [8]

3 Vulnerability details

3.1 Detailed Description

CODESYS products support a routing protocol for the communication between clients (CODESYS Development System, OPC Server, PLCHandler, Remote Target Visu, etc.) and the CODESYS Control runtime system. Crafted communication packets can trigger an out-of-bounds memory buffer access in the communication stack, which may result in a denial-of-service condition.

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

POC is publicly available.

4 Available software updates

CODESYS GmbH has released version V3.5.16.10 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].

It turned out that the previous fix in version V3.5.15.40 was incomplete. Therefore, we recommend an update to V3.5.16.10 to close the vulnerability, regardless of the version used so far.

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
- 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.

We thank Carl Hurd of Cisco Talos, Gao Jian of NSFOCUS and an OEM customer for reporting this vulnerability independently of each other following coordinated disclosure.

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=13077&token=3bfc6d1d08415a6260b96093520071f5786e7fd4&download=

Change History

Version	Description	Date
1.0	First version	10.03.2020
2.0	Affected version corrected	11.03.2020
3.0	Software update available	25.03.2020
4.0	Public POC known	01.04.2020
5.0	Complete revision of the document: Fix for V3.5.15.40 was incomplete, switched to new style sheet	14.07.2020
6.0	Software update available	22.07.2020