Advisory 2021-04

Security update for CODESYS Gateway V3

Published: 30 November 2021

Version: 6.0
Template: templ_tecdoc_en_V3.0.docx
File name: Advisory2021-04_CDS-75011.docx

CONTENT

1 Affected Products

All variants of the following CODESYS V3 products containing the CmpGateway component are affected, regardless of the CPU type or operating system:

- CODESYS Edge Gateway for Linux (all versions affected prior V4.1.0.0)
- CODESYS Control V3 Runtime System Toolkit (all versions affected prior V3.5.16.70)
- CODESYS Development System (all versions affected prior V3.5.16.70)
- CODESYS Edge Gateway for Windows (all versions affected prior V3.5.16.70)
- CODESYS Gateway V3 (all versions affected prior V3.5.16.70)

CmpGateway was removed from the following products with the specified versions below. Therefore, the more recent versions of these products are not affected anymore.

- CODESYS Control for BeagleBone SL (all versions affected prior V4.0.1.0)
- CODESYS Control for emPC-A/iMX6 SL (all versions affected prior V4.0.1.0)
- CODESYS Control for IOT2000 SL (all versions affected prior V4.0.1.0)
- CODESYS Control for Linux SL (all versions affected prior V4.0.1.0)
- CODESYS Control for PFC100 SL (all versions affected prior V3.5.16.0)
- CODESYS Control for PFC200 SL (all versions affected prior V3.5.16.0)
- CODESYS Control for Raspberry Pi SL (all versions affected prior V4.0.1.0)

2 Vulnerability overview

2.1 Type

CWE-476: NULL Pointer Dereference [7]

2.2 Management Summary

Crafted communication requests may cause a Null pointer dereference in the affected CODESYS products and may result in a denial-of-service condition.

2.3 References

CVE: CVE-2021-29241 [6]

CODESYS JIRA: CDS-75011, CDS-77914

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

The CODESYS Gateway routes the online communication between clients like the CODESYS Development System and CODESYS Control runtime systems. As optional component of CODESYS Control runtime systems, it may also run on PLC devices.

Crafted communication requests may cause a Null pointer dereference in the affected CODESYS products and 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

No known public exploits specifically target this vulnerability.

4 Available software updates

CODESYS GmbH has released versions V3.5.16.70 and V3.5.17.0 of the following products. Both versions fix the noted vulnerability.

- CODESYS Control V3 Runtime System Toolkit
- CODESYS Gateway V3
- CODESYS Development System
- CODESYS Edge Gateway for Windows

Furthermore, CODESYS GmbH has released CODESYS Edge Gateway for Linux version V4.1.0.0 based on the CODESYS Control V3 Runtime System Toolkit V3.5.17.0.

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

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 issue was discovered by Uri Katz of Claroty. We thank for reporting it 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=14637&token=8dbd75ae7553ae3be25e22f741db783b31e14799&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
4.0	Further software update available	18.11.2021
5.0	Affected versions adapted	18.11.2021
6.0	Additional JIRA reference added	30.11.2021