Advisory 2021-09

Security update for CODESYS V3 web server

Published: 26 May 2021

Version: 2.0
Template: templ_tecdoc_en_V3.0.docx
File name: Advisory2021-09_CDS-76140.docx

CONTENT

1 Affected Products

In CODESYS V3, the web server is an optional part of the CODESYS runtime system. Therefore, all CODESYS V3 runtime systems containing the CmpWebServer in all versions prior V3.5.17.10 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 (also part of the CODESYS Development System setup)
- CODESYS HMI V3
- CODESYS Control V3 Runtime System Toolkit
- CODESYS V3 Embedded Target Visu Toolkit
- CODESYS V3 Remote Target Visu Toolkit

In addition, the following products based on the CODESYS Control V3 Runtime System Toolkit are affected in all versions prior to V4.2.0.0:

- 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 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

2 Vulnerability overview

2.1 Type

CWE-122: Heap-based Buffer Overflow [7]

2.2 Management Summary

Specific crafted requests may cause a heap-based buffer overflow. Further on this could crash the web server, lead to a denial-of-service condition or may be utilized for remote code execution.

2.3 References

CVE: CVE-2021-33485 [6]

CODESYS JIRA: CDS-76140, CDS-76457, CDS-77136

2.4 Severity Rating

CODESYS GmbH has rated this vulnerability as Critical.

The CVSS v3.0 base score of 9.8 has been assigned. The CVSS vector string is (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H). [8]

3 Vulnerability details

3.1 Detailed Description

The CODESYS web server is used by the CODESYS WebVisu to display CODESYS visualization screens in a web browser. Specific crafted requests may cause a heap-based buffer overflow. Further on this could crash the web server, lead to a denial-of-service condition or may be utilized for remote code execution. As the web server is part of the CODESYS runtime system, this may result in unforeseen behavior of the complete runtime system.

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. However, existing security scanners may cause harm to the affected CODESYS products.

4 Available software updates

CODESYS GmbH has released version V3.5.16.50, which solves the noted vulnerability issue for the following products for versions before V3.5.17.0:

- 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
- CODESYS V3 Embedded Target Visu Toolkit
- CODESYS V3 Remote Target Visu Toolkit

This issue will also be fixed by version V3.5.17.10 of the above products.
The release of version V3.5.17.10 is expected for July 2021.

For the below listed products, the issue will be fixed by version V4.2.0.0, which is based on the CODESYS Control V3 Runtime System Toolkit V3.5.17.10:

- 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 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

The release of version V4.2.0.0 is expected for August 2021.

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

This issue was discovered by Device Security Assurance Center of ABB.

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

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=14805&token=f0b86f99bb302ddd4aadec483aed5f5d3fddbf1a&download=

Change History

Version	Description	Date
1.0	First version	19.05.2021
2.0	Software update available, CVE and further JIRA reference added	26.05.2021