Advisory 2020-03

Security update for CODESYS V3 web server

Published: 01 April 2020

Version: 3.0
Template: templ_tecdoc_en_V2.0.docx
File name: Advisory2020-03_CDS-69655.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 web server (CmpWebServer and CmpWebServerHandler) in all versions prior V3.5.15.40 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 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
• CODESYS V3 Embedded Target Visu Toolkit
• CODESYS V3 Remote Target Visu Toolkit

2 Vulnerability overview

2.1 Type

Heap-based buffer overflow

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-2020-10245 [6]

CODESYS JIRA: CDS-69655, CDS-69672

2.4 Severity Rating

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

The CVSS v3.0 base score of 10.0 has been assigned. The CVSS vector string is (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H). [7]

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 webserver 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

POC is publicly available.

4 Available software updates

3S-Smart Software Solutions GmbH has released version V3.5.15.40 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].

5 Mitigation

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

Currently, 3S-Smart Software Solutions GmbH has not identified any specific workarounds for this vulnerability, in case the software update is not applied.

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.

We thank Tenable, Inc. for reporting this vulnerability 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 3S-Smart Software Solutions support team [5].

8 Disclaimer

3S-Smart Software Solutions 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 3S-Smart Software Solutions GmbH. Insofar as permissible by law, however, none of this information shall establish any guarantee, commitment or liability on the part of 3S-Smart Software Solutions GmbH.

Note: Not all CODESYS features are available in all territories. For more information on geographic restrictions, please contact sales@codesys.com.

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=13078&token=de344ca65252463cc581ef144e0c53bd97b8f211&download=

Change History

Version	Description	Date
1.0	First version	10.03.2020
2.0	Software update available	25.03.2020
3.0	Public POC known	01.04.2020