Advisory 2021-06

Security update for CODESYS Control V2 communication

Published: 25 October 2021

Version: 3.0
Template: templ_tecdoc_en_V3.0.docx
File name: Advisory2021-06_LCDS-348.docx

CONTENT

1 Affected Products

The following CODESYS V2 runtime systems are affected, regardless of the CPU type or operating system:

• CODESYS Runtime Toolkit 32 bit full prior version V2.4.7.55
• CODESYS PLCWinNT prior version V2.4.7.55

2 Vulnerability overview

2.1 Type

CWE-122: Heap-based Buffer Overflow, CWE-121: Stack-based Buffer Overflow, CWE-20: Improper Input Validation [7]

2.2 Management Summary

Crafted requests may cause a heap- or stack-based buffer overflow or a buffer over-read in the affected CODESYS products, resulting in a denial-of-service condition or being utilized for remote code execution.

2.3 References

CVE: CVE-2021-30186, CVE-2021-30188, CVE-2021-30195 [6]

CODESYS JIRA: LCDS-348, LCDS-334, LCDS-338

2.4 Severity Rating

CODESYS GmbH has rated this vulnerability as high.

The CVSS v3.0 base score of 8.8 has been assigned. The CVSS vector string is (CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H). [8]

3 Vulnerability details

3.1 Detailed Description

The CODESYS Control runtime system enables embedded or PC-based devices to be a programmable industrial controller. It provides a communication server for the communication with clients like the CODESYS Development System. This server has the following vulnerabilities:

CVE-2021-30186: CWE-122: Heap-based Buffer Overflow
A crafted request may cause a heap-based buffer overflow in the affected CODESYS products, resulting in a denial-of-service condition.

CVE-2021-30188: CWE-121: Stack-based Buffer Overflow
A crafted request may cause a stack-based buffer overflow in the affected CODESYS products, resulting in a denial-of-service condition or being utilized for remote code execution.

CVE-2021-30195: CWE-20: Improper Input Validation
A crafted request may cause a buffer over-read in the affected CODESYS products, resulting in a denial-of-service condition.

The crafted requests are only processed on the controller, if no online password is configured on the controller or if the attacker has previously successfully authenticated himself at the controller.

3.2 Exploitability

These vulnerabilities could be exploited remotely.

3.3 Difficulty

An attacker with low skills would be able to exploit these vulnerabilities.

3.4 Existence of exploit

No known public exploits specifically target these vulnerabilities.

4 Available software updates

CODESYS GmbH has released the following product versions to solve the noted vulnerability issues for the affected CODESYS products:

• CODESYS Runtime Toolkit 32 bit full version V2.4.7.55
• CODESYS PLCWinNT version V2.4.7.55. This will also be part of the CODESYS Development System setup version V2.3.9.66.

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 vulnerabilities.

Currently, CODESYS GmbH has not identified any specific workarounds for these vulnerabilities, 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

CVE-2021-30186:
This issue was discovered independently of each other by Yossi Reuven of SCADAfence and Sergey Fedonin of Positive Technologies.

CVE-2021-30188:
This issue was discovered independently of each other by Chen Jie of NSFOCUS, and Denis Goryushev and Sergey Fedonin of Positive Technologies.

CVE-2021-30195:
This issue was discovered by Sergey Fedonin and Anton Dorfman of Positive Technologies.

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

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=14725&token=08691519ef764b252630759eff925890176ecd78&download=

Change History

Version	Description	Date
1.0	First version	28.04.2021
2.0	Software update available	11.05.2021
3.0	Researcher added	25.10.2021