Advisory 2021-16

Security update for CODESYS Control V2 TCP/IP communication driver

Published: 25 October 2021

Version: 2.0
Template: templ_tecdoc_en_V3.0.docx
File name: Advisory2021-16_LCDS-361.docx

CONTENT

1 Affected Products

The following CODESYS V2 runtime systems containing the CODESYS TCP/IP communication driver are affected, regardless of the CPU type or operating system:

• CODESYS Runtime Toolkit 32 bit full prior version V2.4.7.56
• CODESYS PLCWinNT prior version V2.4.7.56

2 Vulnerability overview

2.1 Type

CWE-755: Improper Handling of Exceptional Conditions [7]

2.2 Management Summary

Unauthenticated crafted invalid requests are handled insufficiently, resulting in several denial-of-service conditions. Running PLC programs may be stopped, memory may be leaked, or further communication clients may be blocked from accessing the PLC.

2.3 References

CVE: CVE-2021-34593 [6]

CODESYS JIRA: LCDS-361

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 Control runtime system enables embedded or PC-based devices to be a programmable industrial controller. It provides a TCP/IP communication server for the communication with clients like the CODESYS Development System.

An unauthenticated remote attacker can send crafted requests to cause a memory allocation to fail. This condition is only partially handled, which subsequently leads to several denial-of-service conditions. Running PLC programs may be halted, memory can be leaked, or the affected sockets cannot be closed. Thus, an ongoing attack can block all available communication channels of this driver and prevent further clients from accessing the PLC.

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 the following product versions to solve the noted vulnerability issue for the affected CODESYS products:

• CODESYS Runtime Toolkit 32 bit full version V2.4.7.56
• CODESYS PLCWinNT version V2.4.7.56. This will also be part of the CODESYS Development System setup version V2.3.9.68.

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 Steffen Robertz and Gerhard Hechenberger from the SEC Consult Vulnerability Lab.

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=16877&token=8faab0fc1e069f4edfca5d5aba8146139f67a175&download=

Change History

Version	Description	Date
1.0	First version	18.10.2021
2.0	Software update available	25.10.2021