Advisory 2021-08

Security update for CODESYS Control V2 Linux SysFile library implementation

Published: 11 May 2021

Version: 2.0
Template: templ_tecdoc_en_V3.0.docx
File name: Advisory2021-08_LCDS-347.docx

CONTENT

Page

1 Affected Products 3

2 Vulnerability overview 3

2.1 Type 3
2.2 Management Summary 3
2.3 References 3
2.4 Severity Rating 3

3 Vulnerability details 3

3.1 Detailed Description 3
3.2 Exploitability 3
3.3 Difficulty 3
3.4 Existence of exploit 3

4 Available software updates 3

5 Mitigation 4

6 Acknowledgments 4

7 Further Information 4

8 Disclaimer 4

Bibliography 5

Change History 5

1 Affected Products

All runtime systems for Linux based on a CODESYS V2 Runtime Toolkit 32 bit full prior version V2.4.7.55 are affected.

2 Vulnerability overview

2.1 Type

CWE-78: Improper Neutralization of Special Elements used in an OS Command [7]

2.2 Management Summary

The control programmer could use this vulnerability to call additional OS functions from the PLC logic utilizing the SysFile system library.

2.3 References

CVE: CVE-2021-30187 [6]

CODESYS JIRA: LCDS-347

2.4 Severity Rating

CODESYS GmbH has rated this vulnerability as Medium.

The CVSS v3.0 base score of 5.3 has been assigned. The CVSS vector string is (CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:L/I:L/A:L). [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. Control programs can access local or remote IOs, communication interfaces such as serial ports or sockets, and local system functions such as the file system, the real-time clock and other OS functions. The control programmer could use this vulnerability to call additional OS functions via the SysFile system library.

Programming the controller is only possible if no online access password is configured on the controller or if the attacker has previously successfully authenticated himself on the controller.

3.2 Exploitability

PLC programmers could exploit the vulnerability.

3.3 Difficulty

An attacker/programmer 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 CODESYS Runtime Toolkit 32 bit full version V2.4.7.55 to solve the noted vulnerability issue for the affected CODESYS products.

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 Ivan Kurnakov and Sergey Fedonin 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=14727&token=25159b0fc4355f4c6bc2e074a519a9d0cdb23fbb&download=

Change History

Version	Description	Date
1.0	First version	28.04.2021
2.0	Software update available	11.05.2021