CODESYS Control V3 on Linux and QNX operating systems

CODESYS Security Advisory 2023-11

Published: 2024-02-26

1 Overview

On CODESYS Control runtimes running on Linux or QNX operating systems, successfully authenticated PLC programmers can utilize SysFile or CAA-File system libraries to inject calls to additional shell functions.

2 Affected Products

The following products are affected in all versions prior to 3.5.19.50 if they are used on a Linux or QNX operating system:
• CODESYS Runtime Toolkit

The following products are concerned in all versions prior to 4.11.0.0:
• CODESYS Control for BeagleBone SL
• CODESYS Control for emPC-A/iMX6 SL
• CODESYS Control for IOT2000 SL
• CODESYS Control for Linux ARM SL
• CODESYS Control for Linux SL
• CODESYS Control for PFC100 SL
• CODESYS Control for PFC200 SL
• CODESYS Control for PLCnext SL
• CODESYS Control for Raspberry Pi SL
• CODESYS Control for WAGO Touch Panels 600 SL

3 Vulnerability Identifiers, Type and Severity

VDE-2023-066 [1]

CODESYS JIRA: CDS-87209, CDS-87329

CVE-2023-6357 [7]

CWE-78: Improper Neutralization of Special Elements used in an OS Command [8]

CVSS v3.1 Base Score 8.8 | High | CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H [9]

4 Impact

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.

A successfully authenticated control programmer could exploit this vulnerability to inject calls to additional operating system shell functions via the SysFile or CAA file system libraries.

Only CODESYS Control runtime systems running on Linux or QNX operating systems are affected by this vulnerability.

5 Remediation

Update the following products to version 3.5.19.50.
• CODESYS Runtime Toolkit

Update the following products to version 4.11.0.0.
• CODESYS Control for BeagleBone SL
• CODESYS Control for emPC-A/iMX6 SL
• CODESYS Control for IOT2000 SL
• CODESYS Control for Linux ARM SL
• CODESYS Control for Linux SL
• CODESYS Control for PFC100 SL

- CODESYS Control for PFC200 SL
- CODESYS Control for PLCnext SL
- CODESYS Control for Raspberry Pi SL
- CODESYS Control for WAGO Touch Panels 600 SL

The products available as CODESYS add-ons can be downloaded and installed directly with the CODESYS Installer or be downloaded from the CODESYS Store.

Alternatively, as well as for all other products, you will find further information on obtaining the software update in the CODESYS Update area [4].

6 Mitigation

To exploit this vulnerability, a successful login with according user rights to download a PLC application is required. The online user management therefore protects from exploiting this security vulnerability.

CODESYS GmbH strongly recommends using the online user management. This not only prevents an attacker from downloading virulent code or sending malicious requests, but also suppresses starting, stopping, debugging or other actions on a known working application that could potentially disrupt a machine or system. As of version 3.5.17.0, the online user management is enforced by default.

7 General Security Recommendations

As part of a security strategy, CODESYS GmbH strongly recommends at least the following best-practice defense measures:

- 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
- Activate and apply user management and password features
- Limit the access to both development and control system by physical means, operating system features, etc.
- Use encrypted communication links
- Use VPN (Virtual Private Networks) tunnels if remote access is required
- 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 [2].

8 Acknowledgments

This vulnerability was reported by Chuya Hayakawa of 00One, Inc. to JPCERT/CC Vulnerability Coordination Team.

Coordination done by CERT@VDE.

CODESYS GmbH thanks all parties involved for their efforts.

9 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 [6].

10 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.

11 Bibliography

[1] CERT@VDE: https://cert.vde.com

[2] CODESYS GmbH: CODESYS Security Whitepaper

[3] CODESYS GmbH: Coordinated Disclosure Policy

[4] CODESYS GmbH update area: https://www.codesys.com/download

[5] CODESYS GmbH security information page: https://www.codesys.com/security

[6] CODESYS GmbH support contact site: https://www.codesys.com/support

[7] Common Vulnerabilities and Exposures (CVE): https://cve.mitre.org

[8] Common Weakness Enumeration (CWE): https://cwe.mitre.org

[9] CVSS Calculator: https://www.first.org/cvss/calculator/3.1

The latest version of this document can be found here:

https://customers.codesys.com/index.php?eID=dumpFile&t=f&f=18027&token=43109051cf95d3445bc616e4efb8414336ebcc47&download=

Change History

Version	Description	Date
1.0	Initial version	2023-11-29
2.0	Software updates available, CVE and VDE references added	2023-12-05
3.0	Further software updates available	2024-02-26