# Advisory 2022-03

Security update for SysDrv3S

Published: 06 April 2022

Version: 2.0
Template: templ_tecdoc_en_V3.0.docx
File name: Advisory2022-03_CDS-77172.docx

# CONTENT

# 1 Affected Products

The SysDrv3S.sys driver is affected in all versions prior V3.5.18.0. This driver is used on systems with the Microsoft Windows operating system to handle PC fieldbus cards like the Hilscher CIF or CIFX by the following CODESYS V3 products:
• CODESYS Control RTE (SL)
• CODESYS Control RTE (for Beckhoff CX) SL
• CODESYS Control Win (SL)

The driver is delivered as part of the above products and the CODESYS Development System V3 setup.

The SysDrv3S.sys is not automatically installed by running the CODESYS setup, but must be explicitly selected manually during setting up the PC fieldbus card and then installed with admin rights.

Systems on which the affected products were installed without taking these additional steps to install the SysDrv3S.sys driver are not affected by this vulnerability.

CODESYS GmbH is investigating whether further legacy products are concerned.

# 2 Vulnerability overview

## 2.1 Type

CWE-732: Incorrect Permission Assignment for Critical Resource [7]

## 2.2 Management Summary

The SysDrv3S driver allows to map arbitrary physical addresses into the own process space and to access them.

## 2.3 References

CVE: CVE-2022-22516 [6]

CODESYS JIRA: CDS-77172

## 2.4 Severity Rating

CODESYS GmbH has rated this vulnerability as high.

The CVSS v3.1 base score of 7.8 has been assigned. The CVSS vector string is (CVSS:3.1/AV:L/AC:H/PR:L/UI:N/S:C/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. On systems with the Microsoft Windows operating system, the CODESYS Control runtime system uses the SysDrv3S.sys driver to access PC fieldbus cards and thus to be able to address remote IOs. The driver is used to handle Hilscher CIF and CIFX and similar PC fieldbus cards.

The affected versions of the driver allow each user to map arbitrary physical addresses in his own process space. Consequently, any system user can read and write to this memory.

## 3.2 Exploitability

This vulnerability could be exploited locally.

## 3.3 Difficulty

An attacker with high skills would be able to exploit this vulnerability.

### 3.4 Existence of exploit

No known public exploits specifically target this vulnerability in CODESYS products.

## 4 Available software updates

CODESYS GmbH has released version V3.5.18.0 of the driver SysDrv3S.sys and the following product setups containing this new driver version to fix the identified security vulnerability:
• CODESYS Control RTE (SL)
• CODESYS Control RTE (for Beckhoff CX) SL
• CODESYS Control Win (SL)
• CODESYS Development System V3

The CODESYS Development System and the products available as CODESYS AddOns can be downloaded and installed directly with the CODESYS Installer, which is part of the CODESYS Development System as of version V3.5.17.0.

Alternatively, as well as for all other products, you will find further information on obtaining the software update in the CODESYS Update area [3].

To make the fix effective, you have to update the SysDrv3S.sys driver to latest V3.5.18.0 manually:
• In the Microsoft Windows Device Manager right-click on the Hilscher device to open the context menu.
• Select Update driver within this.
• Install the driver from the subdirectory "./Driver" of your CODESYS Development System V3 or CODESYS Control installation directory.
• Check the driver version after the update. The driver must have version number 3.5.18.0.

The SysDrv3S.sys V3.5.18.0 supports the Hilscher PC fieldbus cards only. Thus, the following hardware can no longer be used with the SysDrv3S.sys driver:
• "SysDrv3S Automata CAN PCI 2N" = SysDrv3S, PCI\VEN_10B5&DEV_9050&SUBSYS_34551971”
• "SysDrv3S Peak PCAN-PCI" = SysDrv3S, PCI\VEN_001C&DEV_0001&SUBSYS_0004001C”
• "SysDrv3S Peak PCAN-EXPRESS" = SysDrv3S, PCI\VEN_001C&DEV_0003&SUBSYS_0002001C”

Please contact the CODESYS support [5], if you need to use this driver with one of the PC fieldbus cards listed above or any other currently unsupported hardware.



## 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

The vulnerability was discovered by Denis Goryushev 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



## 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/3.1
[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=17090&token=6cd08b169916366df31388d2e7ba58e7bce93508&download=

## Change History

| Version | Description | Date |
|---|---|---|
| 1.0 | First version | 24.03.2022 |
| 2.0 | Software update available | 06.04.2022 |