Advisory 2022-08

Security Note: Framework for attacks on ICS and SCADA systems (INCONTROLLER / PIPEDREAM)

Published: 14 April 2022

Version: 1.0
Template: templ_tecdoc_en_V3.0.docx
File name: Advisory2022-08_CDS-81389.docx

CONTENT

1 Description

On 13 April 2022, the U.S. agencies CISA, DOE, NSA and FBI published a joint security advisory describing various tools developed for use against industrial control and automation systems. The company Dragos uses the name "PIPEDREAM" and the company Mandiant calls the toolkit "INCONTROLLER.

The ICS-specific framework is modular. It does not exploit specific vulnerabilities, but use standard functions of the CODESYS, MODBUS and OPC UA protocol. The tools of the framework therefore behave like a legitimate client or a development environment for programming the controller.

The framework has the potential for disruption, sabotage, and potentially physical destruction of the controlled machines and processes. Depending on the features used by the tools of the framework and the security features configured on the targeted devices, an attacker may for example perform the following actions:

- Access the OPC UA servers
- Send MODBUS frames to devices
- Perform a network scan
- Connect to a PLC with valid credentials or brute-force the password using the communication protocols
- Download and upload files, PLC applications, configurations, recipes, …
- Execute denial of service attacks

2 Potentially Targeted Products

Potentially all CODESYS V3 products can be targeted that have a communication server for the CODESYS protocol or for OPC UA. These can be all variants and versions of the following CODESYS V3 products regardless of the CPU type or operating system:

- CODESYS Control for BeagleBone SL
- CODESYS Control for Beckhoff CX9020 SL
- CODESYS Control for emPC-A/iMX6 SL
- CODESYS Control for IOT2000 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
- CODESYS Control RTE (SL)
- CODESYS Control RTE (for Beckhoff CX) SL
- CODESYS Control Win (SL)
- CODESYS Gateway
- CODESYS Edge Gateway for Windows
- CODESYS Edge Gateway for Linux
- CODESYS HMI (SL)

Also all OEM customer PLC-products based on the following CODESYS products may be concerned:

- CODESYS Control Runtime System Toolkit
- CODESYS Embedded Target Visu Toolkit
- CODESYS Remote Target Visu Toolkit

Controllers that use the MODBUS protocol may also be targeted. The MODBUS protocol stack is provided as CODESYS library and can be used as part of the IEC application on both CODESYS V2 and CODESYS V3 based controllers.

In addition, other products from other manufacturers are subject to this. See also the references listed below.

3 Mitigation

CODESYS GmbH strongly recommends using the online user management and setup strong passwords. This not only prevents an attacker from sending malicious CODESYS or OPC UA protocol requests or downloading virulent code, but also suppresses starting, stopping, debugging or other actions on a known working application that could potentially disrupt a machine or system.

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

• 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.

• Establish a recovery strategy and test your backups frequently

• Protect both development and control system by using up to date virus detecting and intrusion detection solutions

For more information and general recommendations for protecting machines and plants, see also the CODESYS Security Whitepaper [1].

4 References

BSI: Framework für Angriffe auf ICS- und SCADA-Systeme (INCONTROLLER / PIPEDREAM)
https://www.bsi.bund.de/SharedDocs/Cybersicherheitswarnungen/DE/2022/2022-215481-1032.pdf?__blob=publicationFile&v=2

CISA: Alert (AA22-103A): APT Cyber Tools Targeting ICS/SCADA Devices
https://www.cisa.gov/uscert/ncas/alerts/aa22-103a

Dragos: PIPEDREAM: CHERNOVITE'S EMERGING MALWARE TARGETING INDUSTRIAL CONTROL SYSTEMS
https://hub.dragos.com/hubfs/116-Whitepapers/Dragos_ChernoviteWP_v2b.pdf

Mandiant: INCONTROLLER: New State-Sponsored Cyber Attack Tools Target Multiple Industrial Control Systems
https://www.mandiant.com/resources/incontroller-state-sponsored-ics-tool

Schneider Electric: APT Cyber Tools Targeting ICS/SCADA Devices
https://download.schneider-electric.com/files?p_Doc_Ref=SESB-2022-01

5 Further Information

For additional information regarding the CODESYS products, especially the above-mentioned versions, or about the security note please contact the CODESYS support team [5].

6 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/3.1
[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=17113&token=0c173ece4a2f48bd30d6a67fa2f495119d5caefc&download=

Change History

Version	Description	Date
1.0	First version	14.04.2022