CODESYS Scripting

CODESYS Security Advisory 2023-09

Published: 2023-07-26

1 Overview

CODESYS Scripting executes potentially malicious scripts saved by another user.

2 Affected Products

- CODESYS Development System versions from 3.5.9.0 and before 3.5.17.0
- CODESYS Scripting versions from 4.0.0.0 and before 4.1.0.0

Note: Prior to CODESYS Development System Version 3.5.17.0, CODESYS Scripting was an integral component of the CODESYS Development System. Since CODESYS Development System version 3.5.17.0, CODESYS Scripting is provided as an optional add-on and can be updated separately. The first add-on version of CODESYS Scripting was version 4.0.0.0.

3 Vulnerability Identifiers, Type and Severity

VDE-2023-024 [1]

CODESYS JIRA: SCRIPT-44

CVE-2023-3670 [7]

CWE-668: Exposure of Resource to Wrong Sphere [8]

CVSS v3.1 Base Score 7.3 | High | CVSS:3.1/AV:L/AC:L/PR:L/UI:R/S:U/C:H/I:H/A:H [9]

4 Impact

The CODESYS Development System is an IEC 61131-3 programming tool for the industrial controller and automation technology sector. As an add-on to the CODESYS Development System, CODESYS Scripting allows to automate commands or complex program sequences in CODESYS that otherwise require manual mouse clicks and text input in the CODESYS user interface. For this purpose, scripts based on (Iron)Python can be started from the CODESYS user interface or from the Windows command line.

The scripts can be executed either from the installation directory, which is secured by default with administrator privileges, or from subfolders of "%PROGRAMDATA%\CODESYS\". The last one is writable for all low privilege users, so that another user can store here potentially harmful scripts. CODESYS Scripting offers all available scripts for execution, so the legitimate user may then execute malicious scripts.

5 Remediation

Update CODESYS Scripting to version 4.1.0.0.

This version can be downloaded and installed directly with the CODESYS Installer. A CODESYS Development System version of 3.5.17.0 or newer is required.

Alternatively, you can visit the CODESYS update area for more information on how to obtain the software update [4].

CODESYS Scripting 4.1.0.0 and later no longer uses the "%PROGRAMDATA%\CODESYS\Script Commands" and "%PROGRAMDATA%\CODESYS\ScriptDir" folders as a source for scripts. Instead, the folders "C:\Users\<user>\AppData\CODESYS\Script Commands" and "C:\Users\<user>\AppData\CODESYS\ScriptDir" are used. The handling of scripts stored in the installation folder remains unchanged.

6 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].

7 Acknowledgments

This vulnerability was discovered by Sina Kheirkhah (@SinSinology) of Summoning Team (@SummoningTeam) working with Trend Micro Zero Day Initiative.

Coordination done by CERT@VDE.

CODESYS GmbH thanks all parties involved for their efforts.

8 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].

9 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.

10 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=17769&token=a1a34cd304aebfbc1e2619e401a9a6cb5d4dc117&download=

Change History

Version	Description	Date
1.0	Initial version	2023-07-20
2.0	Software update available	2023-07-26