Advisory 2021-13

Security update for CODESYS Development System V3 including CODESYS Installer and CODESYS SVN

Published: 27 July 2022

Version: 6.0

Template: templ_tecdoc_en_V3.0.docx

File name: Advisory2021-13_CDS-77365.docx

CONTENT

1 Affected Products

Both the 32-bit and 64-bit variants of the following CODESYS V3 products are affected by one or more of the vulnerabilities described below:

- CODESYS Development System prior version V3.5.17.10
- CODESYS Installer prior version V1.3.0
- CODESYS SVN prior version V4.4.0.0

The affected versions of the CODESYS Installer were shipped as part of the CODESYS Development System V3 setup from V3.5.17.0 and before V3.5.18.20.

CODESYS SVN is part of the CODESYS Professional Developer Edition add-on bundle.

2 Vulnerability overview

2.1 Type

CWE-502: Deserialization of Untrusted Data [7]

2.2 Management Summary

The CODESYS Development System V3, the CODESYS Installer and CODESYS SVN deserialize local configuration and profile files, parts of the CODESYS project and CODESYS project archive files without sufficiently verifying the data.

2.3 References

CVE: CVE-2021-21863, CVE-2021-21864, CVE-2021-21865, CVE-2021-21866, CVE-2021-21867, CVE-2021-21868, CVE-2021-21869 [6]

CODESYS JIRA: CDS-77365, CDS-77156, CDS-77359, CDS-77364, CDS-77561, CDS-77562, INST-163, SVN-914

2.4 Severity Rating

CODESYS GmbH has rated this vulnerability as high.

The CVSS v3.0 base score of 8.8 has been assigned. The CVSS vector string is (CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H). [8]

3 Vulnerability details

3.1 Detailed Description

The CODESYS Development System is an IEC 61131-3 programming tool for the industrial controller and automation technology sector. The CODESYS Installer manages the local installation of different CODESYS Development System V3 versions and supports their deployment and update. CODESYS SVN is an add-on providing an SVN version control client integrated into the CODESYS Development system. All three products are affected by several vulnerabilities:

CVE-2021-21863:
CODESYS Development System V3 versions prior V3.5.17.10 and CODESYS Installer versions prior V1.3.0 deserialize local profile files without sufficiently verifying the data.

CVE-2021-21864:
CODESYS Development System V3 versions prior V3.5.17.10 deserialize local configuration files without sufficiently verifying the data.

CVE-2021-21865, CVE-2021-21866, CVE-2021-21867, CVE-2021-21868, CVE-2021-21869:
CODESYS Development System V3 versions prior to version V3.5.17.10 deserialize various parts of CODESYS project and CODESYS repository files without sufficiently verifying the data. CODESYS SVN versions prior to version V4.4.0.0 deserialize CODESYS project artifacts received from SVN repositories without sufficiently verifying the data.

An attacker who successfully leverages these vulnerabilities can cause a denial of service (DoS), information disclosure, or remote code execution in affected CODESYS products. To exploit these vulnerabilities, an attacker must either modify local configuration and profile files of the CODESYS installation or make the local user to open a malicious CODESYS project or archive. Installing malicious packages utilizing the CODESYS package manager can also modify or add affected files. In the case of CODESYS SVN, accessing an SVN repository that contains malicious CODESYS project artifacts (storage profile) can trigger an attack when parsing the objects.

3.2 Exploitability

The vulnerabilities could be exploited by modifying the CODESYS installation or with the help of local users.

3.3 Difficulty

An attacker with low skills would be able to exploit these vulnerabilities.

3.4 Existence of exploit

POCs are publicly available.

4 Available software updates

CODESYS GmbH has released the following versions of the concerned CODESYS products to solve the noted vulnerability issues:

- CODESYS Development System V3.5.17.10
- CODESYS Installer V1.3.0
- CODESYS SVN V4.4.0.0

All CODESYS Development System V3 versions prior to V3.5.17.10 should be replaced by version V3.5.18.20 to ensure the fix for the CODESYS Development System and also for the CODESYS Installer is maintained.

For CODESYS Development System V3 versions from V3.5.17.10 and before V3.5.18.20, it is sufficient for the fix to run the CODESYS Installer in order to update it to V1.3.0 and keep the CODESYS Development System version(s).

After the update of the CODESYS Development System V3 and/or CODESYS installer, version V4.4.0.0 of CODESYS SVN can be downloaded and installed directly with the CODESYS Installer.

The CODESYS Development System V3 can be downloaded and installed directly with the CODESYS Installer or downloaded from the CODESYS Store. The CODESYS Installer checks for available updates at every startup and provides an update feature to update itself automatically.

Alternatively, you will find further information on obtaining the software update in the CODESYS Update area [3].

5 Mitigation

CODESYS GmbH recommends using the available software updates to fix the vulnerabilities.

CODESYS GmbH has currently found no workaround for these vulnerabilities. Therefore, you should protect your CODESYS installation from unknown access and only open/install CODESYS archives, projects and packages from trustworthy sources, in case the software update is not applied.

CODESYS SVN users should avoid connecting to unknown / untrusted SVN servers, or servers with untrusted users, in order to prevent loading of malicious CODESYS project artifacts.

Note: As of version V3.5.17.0, the CODESYS package manager checks the signature of the packages before installation. Since then, CODESYS GmbH has only provided signed packages.

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

These issues were discovered by Patrick DeSantis of Cisco Talos.

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.govhttps://ics-cert.us-cert.gov/advisories/ICSA-15-288-01

The latest version of this document can be found here:

https://customers.codesys.com/index.php?eID=dumpFile&t=f&f=16805&token=ee583c498941d9fda86490bca98ff21928eec08a&download=

Change History

Version	Description	Date
1.0	First version	15.07.2021
2.0	Software update available, CVSS rating adjusted	22.07.2021
3.0	POC publicly available	02.08.2021
4.0	CODESYS Installer also affected, Software update available	30.05.2022
5.0	Software versions adapted, as V3.5.18.10 was withdrawn	03.06.2022

6.0	CODESYS SVN also affected, Software update available	27.07.2022

Template: templ_tecdoc_en_V3.0.docx