Advisory 2021-13

Security update for CODESYS Development System V3

Published: 02 August 2021

Version: 3.0
Template: templ_tecdoc_en_V3.0.docx
File name: Advisory2021-13_CDS-77365.docx

CONTENT

1 Affected Products

All CODESYS Development System V3 versions prior V3.5.17.10 are affected by this vulnerability. This applies to both the 32-bit and 64-bit variants.

2 Vulnerability overview

2.1 Type

CWE-502: Deserialization of Untrusted Data [7]

2.2 Management Summary

The CODESYS Development System deserializes 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

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 Development System deserializes local configuration and profile files, parts of the CODESYS project and CODESYS project archive files without sufficiently verifying the data. 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.

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

POC is publicly available.

4 Available software updates

CODESYS GmbH has released version V3.5.17.10 to solve the noted vulnerability issue for all affected products.

Please visit the CODESYS update area for more information on how to obtain the software update [3].

5 Mitigation

CODESYS GmbH recommends using the available software update to fix the vulnerability.

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.

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.gov

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