Advisory 2021-10

Security update for CODESYS V3 Runtime Toolkit for VxWorks

Published: 22 July 2021

Version: 3.0
Template: templ_tecdoc_en_V3.0.docx
File name: Advisory2021-10_CDS-76136.docx

CONTENT

		Page
1	**Affected Products**	**3**
2	**Vulnerability overview**	**3**
2.1	Type	3
2.2	Management Summary	3
2.3	References	3
2.4	Severity Rating	3
3	**Vulnerability details**	**3**
3.1	Detailed Description	3
3.2	Exploitability	3
3.3	Difficulty	3
3.4	Existence of exploit	3
4	**Available software updates**	**4**
5	**Mitigation**	**4**
6	**Acknowledgments**	**4**
7	**Further Information**	**4**
8	**Disclaimer**	**4**
Bibliography		**5**
Change History		**5**

1 Affected Products

All versions of the CODESYS V3 Runtime Toolkit for VxWorks from version V3.5.8.0 and before version V3.5.17.10 are affected.

2 Vulnerability overview

2.1 Type

CWE-755: Improper Handling of Exceptional Conditions [7]

2.2 Management Summary

The platform adaptation layer of the CODESYS V3 Runtime Toolkit for VxWorks does not handle a shortage of sockets correctly, so that existing socket connections may be disconnected and cannot be re-established for some time.

2.3 References

CVE: CVE-2021-33486 [6]

CODESYS JIRA: CDS-76136, CDS-74959, CDS-76459, CDS-76460, CDS-77137

2.4 Severity Rating

CODESYS GmbH has rated this vulnerability as high.

The CVSS v3.0 base score of 7.5 has been assigned. The CVSS vector string is (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/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. In order to run on different operating systems, it includes a platform adaptation layer. The adaptation layer for VxWorks does not handle a shortage of sockets correctly, so that existing socket connections may be disconnected and cannot be re-established for some time. This vulnerability affects various communication servers in the CODESYS V3 Runtime Toolkit for VxWorks such as OPC UA or the UDP communication driver and others.

3.2 Exploitability

This vulnerability could be exploited remotely.

3.3 Difficulty

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

3.4 Existence of exploit

No known public exploits specifically target this vulnerability in CODESYS products. However, existing security scanners may cause harm to the affected CODESYS products.

4 Available software updates

CODESYS GmbH has released versions V3.5.16.50 and V3.5.17.10, which both fix the identified security vulnerability for the affected product.

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.

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

This issue was discovered by Device Security Assurance Center of ABB.

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=14806&token=637e12e86301b83beac1653bd88da3aa5aa3f51b&download=

Change History

Version	Description	Date
1.0	First version	19.05.2021
2.0	Software update available, CVE and further JIRA reference added	26.05.2021
3.0	Further software update available	22.07.2021