Advisory 2017-03

Security update for various CODESYS V3 products using the CODESYS communication protocol

Published: July 13, 2017

Version: 2.0
Template: templ_tecdoc_en_V2.0.docx
File name: Advisory2017-03_CDS-51933.docx

CONTENT

1 Affected Products

The following CODESYS V3 products in all versions prior V3.5.11.0 are affected, regardless of the CPU type or operating system:

- CODESYS Control V3 Runtime System Toolkit
- CODESYS V3 Embedded Target Visu Toolkit
- CODESYS V3 Remote Target Visu Toolkit
- CODESYS Control for BeagleBone
- CODESYS Control for emPC-A/iMX6
- CODESYS Control for PFC200
- CODESYS Control for Raspberry Pi
- CODESYS Control RTE V3 (all variants)
- CODESYS Control Win V3 (all variants)
- CODESYS Gateway V3
- CODESYS HMI V3
- CODESYS OPC Server V3 (all variants)
- CODESYS PLCHandler SDK
- CODESYS V3 Remote Target Visu (all variants)
- CODESYS V3 Safety SIL2
- CODESYS V3 Safety SIL2 PSP
- CODESYS V3 Simulation Runtime (part of the CODESYS IDE)

2 Vulnerability overview

2.1 Type

Access violation, remote DoS

2.2 Management Summary

A crafted request may cause an access violation in the affected CODESYS products and may result in a denial-of-service condition.

2.3 References

CODESYS JIRA: CDS-51933, CDS-52677, CDS-53086

2.4 Severity Rating

3S-Smart Software Solutions GmbH has rated this vulnerability as high.

The CVSS v3 base score of 7.5 has been assigned. The CVSS 3.0 vector string is (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H). [7]

3 Vulnerability details

3.1 Detailed Description

If an affected CODESYS product receives such a crafted request, it may run into an access violation of the communication thread and/or end up in a denial-of-service condition. The crafted request may be sent directly addressed or as CODESYS communication broadcast using one of the available CODESYS communication drivers (e. g. for UDP, TCP, USB, serial line, CANopen, ...) to an affected device to harm it.

3.2 Exploitability

This vulnerability could be exploited remotely.

3.3 Difficulty

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

3.4 Existence of exploit

No known public exploits specifically target this vulnerability.

4 Available software updates

3S-Smart Software Solutions GmbH has released version V3.5.11.0, which solves the noted vulnerability issue for all affected CODESYS products [3].

5 Mitigation

3S-Smart Software Solutions GmbH has not identified any workarounds for this vulnerability.

But 3S-Smart Software Solutions GmbH recommends as part of the mitigation strategy the following defensive measures to reduce the risk of exploitation of this vulnerability:

- 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
- Protect both development and control system from unauthorized access e. g. by means of the operating system
- 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

3S-Smart Software Solutions GmbH thanks those in the security community, who help us to improve our products and to protect customers and users through coordinated vulnerability disclosure.

This vulnerability was reported internally by the CODESYS Security Team.

7 Further Information

For additional information regarding the CODESYS products, especially the above mentioned versions, or about the described vulnerability please contact the 3S-Smart Software Solutions support team [5].

8 Disclaimer

3S-Smart Software Solutions 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 3S-Smart Software Solutions GmbH. Insofar as permissible by law, however, none of this information shall establish any guarantee, commitment or liability on the part of 3S-Smart Software Solutions GmbH.

Note: Not all CODESYS features are available in all territories. For more information on geographic restrictions, please contact support@codesys.com.

Bibliography

[1] 3S-Smart Software Solutions GmbH: CODESYS Security Whitepaper
[2] 3S-Smart Software Solutions GmbH: Coordinated Disclosure Policy
[3] 3S-Smart Software Solutions GmbH download area: https://www.codesys.com/download
[4] 3S-Smart Software Solutions GmbH security information page: https://www.codesys.com/security
[5] 3S-Smart Software Solutions GmbH support contact site: https://www.codesys.com/support-training
[6] Common Vulnerabilities and Exposures (CVE): https://cve.mitre.org
[7] CVSS Calculator: https://www.first.org/cvss/calculator/3.0
[8] ICS-CERT: https://ics-cert.us-cert.gov

The latest version of this document can be found here:

https://customers.codesys.com/fileadmin/data/customers/security/2017/Advisory2017-03_CDS-51933.pdf

Change History

Version	Description	Date
1.0	First version	30.05.2017
2.0	Software update available	13.07.2017