Advisory 2017-06

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

Published: July 13, 2017

Version: 2.0
Template: templ_tecdoc_en_V2.0.docx
File name: Advisory2017-06_CDS-54740.docx

© 3S-Smart Software Solutions GmbH

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 4

3.1 Detailed Description 4
3.2 Exploitability 4
3.3 Difficulty 4
3.4 Existence of exploit 4

4 Available software updates 4

5 Mitigation 4

6 Acknowledgments 5

7 Further Information 5

8 Disclaimer 5

Bibliography 6

Change History 6

1 Affected Products

All CODESYS V3 products prior version V3.5.11.0, containing the CmpBlkDrvUdp and running on top of one of the following operating systems are affected:

- Linux
- VxWorks
- WindowsCE

Further on we expect that CODESYS based products running on bare metal controllers using embedded Ethernet stacks or running on top of other operating systems than Microsoft Windows, may also be affected. CODESYS products running on Microsoft Windows desktop and server operating systems are not concerned by this issue.

The products below contain the CmpBlkDrvUdp and are available at least for one of the affected or likely affected platforms above:

- CODESYS Control V3 Runtime System Toolkit
- CODESYS V3 Embedded Target Visu Toolkit
- CODESYS V3 Remote Target Visu Toolkit
- CODESYS Gateway V3
- CODESYS PLCHandler SDK
- CODESYS V3 Remote Target Visu (all variants)
- CODESYS V3 Safety SIL2
- CODESYS V3 Safety SIL2 PSP

The products below contain the CmpBlkDrvUdp and run on an affected platform:

- CODESYS Control for BeagleBone
- CODESYS Control for emPC-A/iMX6
- CODESYS Control for PFC200
- CODESYS Control for Raspberry Pi
- CODESYS OPC Server V3 for WindowsCE

Template: templ_tecdoc_en_V2.0.docx

2 Vulnerability overview

2.1 Type

Remote DoS

2.2 Management Summary

A crafted UDP packet may block further CODESYS UDP communication between clients (e. g. CODESYS IDE, OPC Server) and the CODESYS Control Runtime System.

2.3 References

CODESYS JIRA: CDS-54740, CDS-54760

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

CODESYS products support several protocols for the communication between clients (CODESYS IDE, OPC Server, PLCHandler, Remote Target Visu, etc.) and the CODESYS Runtime System. Among the various drivers for the specific medias (e. g. CAN, Serial Line, TCP, UDP, USB, ...) the UDP communication driver is affected by this vulnerability. A crafted UDP packet may block further UDP communication of all affected products containing the CmpBlkDrvUdp.

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. But existing security scanners may cause harm to the affected CODESYS products.

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].

For the following products 3S-Smart Software Solutions GmbH provides the fix also in patch version V3.5.10.50:

- CODESYS Control V3 Runtime System Toolkit
- CODESYS V3 Embedded Target Visu Toolkit
- CODESYS V3 Remote Target Visu Toolkit

5 Mitigation

For the CmpBlkDrvUdp 3S-Smart Software Solutions GmbH has not identified any workarounds for this vulnerability. As other communication block drivers are not affected by this issue, they can be used instead. Especially the CmpBlkDrvTcp could be an alternative for PLCs connected by Ethernet.

To communicate via the CmpBlkDrvTcp you have to configure the IP address of the PLC within the communication parameters instead of using the network scan results or the PLC node name.

Further on 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].

Template: templ_tecdoc_en_V2.0.docx

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.

We thank the Security Team at Eurotherm by Schneider Electric for reporting this vulnerability following coordinated disclosure.

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/Advisory2017-06_CDS-54740.pdf

Change History

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

© 3S-Smart Software Solutions GmbH