



**CODESYS**

## **Advisory 2017-01**

CODESYS V3

Security update for CODESYS Control V3 OPC UA Server

Published: April 28, 2017

Version: 3.0

Template: templ\_tecdoc\_en\_V2.0.docx

File name: Advisory2017-01\_CDS-53070.docx

# CONTENT

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

## 1 Affected Products

All CODESYS Control V3 Runtime Systems containing an OPC UA Server prior version V3.5 SP10 Patch 2 are affected. The CODESYS OPC UA Server was initially released with version V3.5 SP6 Patch 2. Beside the CODESYS Control V3 Runtime System Toolkit, the following products are affected by this issue:

- CODESYS Control for BeagleBone
- CODESYS Control for emPC-A/iMX6
- CODESYS Control for PFC200
- CODESYS Control for Raspberry Pi
- CODESYS Control RTE (all variants)
- CODESYS Control Win

## 2 Vulnerability overview

### 2.1 Type

Remote DoS

### 2.2 Management Summary

The CODESYS OPC UA server does not recover from a remote DoS attack.

### 2.3 References

CODESYS JIRA: CDS-53070

### 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 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

The CODESYS OPC UA Server is an optional part of the runtime system. The CODESYS OPC UA Server is used to exchange data between the runtime system and OPC UA clients like SCADA or HMIs.

The CODESYS OPC UA server does not recover from a remote DoS attack. Further on existing client connections may be disturbed in timing or interrupted due to this vulnerability.

The availability of other communication servers of the runtime (e.g. CODESYS online communication or the web visualization) is not affected by this issue.

### 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 the CODESYS OPC UA Server.

## 4 Available software updates

3S-Smart Software Solutions GmbH has released version V3.5 SP10 Patch 2 for all affected CODESYS products to solve this vulnerability issue.

## 5 Mitigation

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

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

- 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

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.

## 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/Advisory2017-01\\_CDS-53070.pdf](https://customers.codesys.com/fileadmin/data/customers/security/2017/Advisory2017-01_CDS-53070.pdf)

## Change History

Version	Description	Date
1.0	First version	23.02.2017
2.0	Software update available	14.03.2017
3.0	Formal rework	28.04.2017