Advisory 2018-04

Security update for CODESYS V2 and V3 runtime systems

Published: 11 July 2018

Version: 4.0
Template: templ_tecdoc_en_V2.0.docx
File name: Advisory2018-04_CDS-59017.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	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 Control V3 runtime systems prior version V3.5.12.30 containing the CmpFiletransfer component are affected, regardless of the CPU type or operating system:
• CODESYS Control for BeagleBone
• CODESYS Control for emPC-A/iMX6
• CODESYS Control for IOT2000
• CODESYS Control for PFC100
• CODESYS Control for PFC200
• CODESYS Control for Raspberry Pi
• CODESYS Control RTE V3 (all variants)
• CODESYS Control Win V3 (all variants)
• CODESYS V3 Simulation Runtime (part of the CODESYS Development System)
• CODESYS HMI V3 (all variants)
• CODESYS V3 Remote Target Visu (all variants)
• CODESYS Control V3 Runtime System Toolkit
• CODESYS V3 Embedded Target Visu Toolkit
• CODESYS V3 Remote Target Visu Toolkit

Furthermore also the following legacy CODESYS V2 runtime systems supporting PLC-Browser or file transfer online services are affected, regardless of the CPU type or operating system:
• CODESYS Runtime Toolkit 32 bit embedded prior version V2.3.2.10
• CODESYS Runtime Toolkit 32 bit full prior version V2.4.7.52
• CODESYS Runtime PLCWinNT prior version V2.4.7.52

2 Vulnerability overview

2.1 Type

Directory traversal

2.2 Management Summary

The CODESYS runtime system allows to access files outside the restricted working directory of the controller by online services.

2.3 References

CODESYS JIRA: CDS-59017, LCDS-285, LCDS-286, CDS-59793, CDS-59795

2.4 Severity Rating

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

The CVSS v3.0 base score of 9.9 has been assigned. The CVSS vector string is (CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:C/C:H/I:H/A:H). [7]

3 Vulnerability details

3.1 Detailed Description

The CODESYS runtime system enables embedded or PC-based devices to be a programmable industrial controller. For the communication with the CODESYS Development System, the implemented CODESYS protocol provides also access to the files or directories located underneath a restricted parent directory system of the controller. However, by default the software does not properly resolve the received online service to deny access to locations outside the restricted directory. Depending on the operating system and user context, in which the CODESYS runtime system is executed, all system files or only the files (including network shares) of the user context can be accessed.

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, but there exist features in CODESYS and customer specific products, which can potentially be used to access files outside the restricted working directory of the controller.

4 Available software updates

CODESYS V3:

3S-Smart Software Solutions GmbH has released versions V3.5.11.60, V3.5.12.30 and V3.5.13.0 to solve the noted vulnerability issue for all affected CODESYS products.

CODESYS V2:

3S-Smart Software Solutions GmbH has released the following versions to solve the noted vulnerability issue for all affected CODESYS V2 products:
- CODESYS Runtime Toolkit 32 bit embedded version V2.3.2.10
- CODESYS Runtime Toolkit 32 bit full version V2.4.7.52
- CODESYS Runtime PLCWinNT version V2.4.7.52. This is also part of the CODESYS Development System setup version V2.3.9.57.

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

Compatibility note:

To fix the vulnerability, the CODESYS runtime systems restrict all online file accesses to the standard path and its subdirectories. CODESYS V3 runtime systems additionally allow the online file access to all configured file and placeholder file paths and deny the online access to all runtime configuration files, independently of the location.

If access to other directories or files is needed and the security requirements are fulfilled by other means, PLC vendors are able to grant access by specific runtime system configurations or software hooks. In this case, a careful threat analysis is advisable.

However, 3S-Smart Software Solutions GmbH strictly recommends keeping the new default access restrictions.

Additonal information for OEM customers using one of these toolkits:

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

The fix versions V3.5.11.60 and V3.5.12.30 of the toolkits above are only suitable, if the CmpUserMgr is included into the runtime system. Customer products without the CmpUserMgr should upgrade to V3.5.12.50 or V3.5.13.0 of the appropriate toolkit.

5 Mitigation

3S-Smart Software Solutions GmbH has identified the following mitigations for this vulnerability:

1. Activation of the controller’s user management or online access password
With the activation of the user management on the device any online service requires an appropriate

authentication. It is highly recommended to setup at least one administrator user. Moreover, a set of users belonging to the appropriate groups allow maintaining leveled access rights. Instead of the user management of CODESYS V3, the CODESYS V2 runtime systems provide an online access password only.

2. Activation of ForceFilePath
CODESYS V3 runtime systems only: In general a PLC vendor is able to restrict the file path settings in the section [SysFile] with "ForceFilePath=1". This setting restricts all file accesses of the CODESYS runtime system including IEC application code and online services to the standard path and its subdirectories.
In addition, since V3.5.8.0 the "FilePath" and "PlaceholderFilePath" settings allow file access to further locations as well. This makes this restriction customizable and the remaining file system is securely locked.

For more information, please refer to the tutorial "FilePath & Placeholders" (CODESYSControlV3_FilePath_Placeholders.pdf) as part of the runtime toolkit documentation.

3. File access restriction by means of the operating system
Furthermore a read-only file system or partition may provide additional security to system files and configurations.

In general 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
• Activate and apply user management and password features
• 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

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 Prosoft-Systems Ltd. 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 sales@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 CODESYS update 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
[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/2018/Advisory2018-04_CDS-59017.pdf

Change History

Version	Description	Date
1.0	First version	22.03.2018
2.0	List of affected products corrected, software update available	20.04.2018
3.0	List of affected products extended, further software update available	26.04.2018
4.0	Further software update available, compatibility note for OEM customers added, link to support contact site adapted	09.07.2018