Advisory 2018-12

Security update for CODESYS Development System V3 compiled libraries

Published: 17 December 2018

Version: 2.0
Template: templ_tecdoc_en_V2.0.docx
File name: Advisory2018-12_CDS-60637.docx

CONTENT

1 Affected Products

All CODESYS Development System V3 versions prior V3.5.14.0 are affected by this vulnerability. This applies to both the 32-bit and 64-bit variants.

2 Vulnerability overview

2.1 Type

File Information Exposure

2.2 Management Summary

Compiled libs created by affected CODESYS Development systems may contain some information of internal objects.

2.3 References

CODESYS JIRA: CDS-60637, CDS-60639, CDS-61649

2.4 Severity Rating

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

The CVSS v3.0 base score of 4.0 has been assigned. The CVSS vector string is (CVSS:3.0/AV:L/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N). [7]

3 Vulnerability details

3.1 Detailed Description

The CODESYS Development System is an IEC 61131-3 programming tool for the industrial controller and automation technology sector. Parts of the application source code can be stored in source or compiled libraries. Compiled libraries do not contain source code, only compiled objects. The affected versions of the CODESYS Development System may add some information of internal objects to the compiled libs.

3.2 Exploitability

This vulnerability could be exploited by accessing the compiled library file.

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.

4 Available software updates

3S-Smart Software Solutions GmbH has released version V3.5.14.0 to solve the noted vulnerability issue for all affected CODESYS products.

In order to benefit from the fix, compiled libraries have to be recompiled from the source libraries using a CODESYS Development System version V3.5.14.0 or higher. An update of the compiler version is not necessary.

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

OEM compatibility information:
Objects that implement ILanguageModelProvider2 and return true for the property NeedsContextForLanguageModelProvision were so far always included in compiled libraries, independent of the value for the build property "Exclude from build".
This behavior changes from V3.5.14.0 onwards. The object will not be saved in the compiled library anymore. So if any of the information contained in the object is still required to be stored in the compiled library the "Exclude from build" option must not be used anymore for this kind of objects.

5 Mitigation

Currently, 3S-Smart Software Solutions GmbH has not identified any workarounds for this vulnerability.
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 Heinz Füglister of WRH Walter Reist Holding AG 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/Advisory2018-12_CDS-60637.pdf

Change History

Version	Description	Date
1.0	First version	06.12.2018
2.0	Software update available	17.12.2018