Advisory 2019-05

Security update for CODESYS V3 Library Manager

Published: 18 December 2019

Version: 4.0
Template: templ_tecdoc_en_V2.0.docx
File name: Advisory2019-05_CDS-62029.docx

CONTENT

1 Affected Products

All CODESYS Development System V3 versions prior V3.5.15.0 are affected by this vulnerability. This applies to both the 32-bit and 64-bit variants.

2 Vulnerability overview

2.1 Type

Cross-site Scripting (XSS)

2.2 Management Summary

The CODESYS Development System may display or execute malicious active contents of the library documentation without first checking the validity.

2.3 References

CVE: CVE-2019-13538 [6]

ICS-CERT: ICSA-19-255-02 [8]

CODESYS JIRA: CDS-62029

2.4 Severity Rating

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

The CVSS v3.0 base score of 8.6 has been assigned. The CVSS vector string is (CVSS:3.0/AV:L/AC:L/PR:N/UI:R/S:C/C:H/I:H/A:H). [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. The source code of CODESYS projects or parts of it can be packaged into compiled libraries to pass this code on or use it in other projects. Documentation is an elementary part of the CODESYS libraries. In addition to the usually chosen straight representation of the documentation, the documentation can also be enriched with active contents. Since the CODESYS Development System tries to display these without checking the validity, malicious contents of manipulated libraries may also be displayed or executed. The issue exits also for source libraries but 3S-Smart Software Solutions GmbH strongly recommends distributing compiled libraries only.

3.2 Exploitability

This vulnerability could be exploited by or with the help of local users.

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 V3.5.15.0 to solve the noted vulnerability issue for all affected CODESYS products.

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

After applying the software update, JavaScript included in the library documentation is only executed, if the library was correctly signed with a valid certificate.

5 Mitigation

3S-Smart Software Solutions GmbH recommends using the available software update to fix the vulnerability.

3S-Smart Software Solutions GmbH has currently found no workaround for this vulnerability. Therefore, you should only install and use CODESYS libraries from trustworthy sources, in case the software update is not applied.

As part of a security strategy, 3S-Smart Software Solutions GmbH recommends the following general defense measures to reduce the risk of exploits:
• 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/2019/Advisory2019-05_CDS-62029.pdf

Change History

Version	Description	Date
1.0	First version	22.07.2019
2.0	Typo corrected	22.07.2019
3.0	Software update available	29.07.2019
4.0	CVE and public reference added	18.12.2019