Advisory 2018-06

Security update for CODESYS Control V3 and CODESYS HMI V3 - OpenSSL update

Published: 11 July 2018

Version: 2.0
Template: templ_tecdoc_en_V2.0.docx
File name: Advisory2018-06_CDS-53155.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	**Further References**	**4**
6	**Mitigation**	**4**
7	**Acknowledgments**	**4**
8	**Further Information**	**4**
9	**Disclaimer**	**5**
Bibliography		**6**
Change History		**6**

1 Affected Products

All CODESYS Control V3 Runtime Systems prior version V3.5.13.0 containing the CmpOpenSSL component are affected, regardless of the CPU type or operating system. The CmpOpenSSL was initially released with version V3.5.5.0. The following products are concerned by this issue:
- 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 - also part of the CODESYS setup)
- 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

2 Vulnerability overview

2.1 Type

DoS, remote DoS

2.2 Management Summary

This advisory addresses the update of OpenSSL to version 1.0.2o to fix known OpenSSL vulnerabilities.

2.3 References

CVE: CVE-2017-3735, CVE-2018-0739 (for vulnerabilities in OpenSSL) [6]

CODESYS JIRA: CDS-53155

2.4 Severity Rating

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

The CVSS v3.0 base score of 5.3 has been assigned. The CVSS vector string is (CVSS:3.0/AV:N/AC:H/PR:L/UI:N/S:U/C:N/I:N/A:H). [7]

3 Vulnerability details

3.1 Detailed Description

The CODESYS Control Runtime System enables embedded or PC-based devices to be a programmable industrial controller. The CmpOpenSSL component adds the OpenSSL cryptographic software library to the CODESYS Runtime Systems. It is used for certificate management, encrypted communication, boot project signing and encryption and is also provided for general purpose by the IEC code.

The following OpenSSL vulnerabilities concern the listed CODESYS products:
- CVE-2017-3735 (Malformed X.509 IPAddressFamily could cause OOB read): The OpenSSL development team rated this vulnerability as low.
- CVE-2018-0739 (Constructed ASN.1 types with a recursive definition could exceed the stack): The OpenSSL development team rated this vulnerability as moderate.

This advisory addresses the update of OpenSSL to version 1.0.2o to fix the known OpenSSL vulnerabilities. Please see the OpenSSL advisories for more information.

3.2 Exploitability

This vulnerability could be exploited remotely.

3.3 Difficulty

An attacker with high 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 V3.5.13.0 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].

5 Further References

OpenSSL Security Advisories:
https://www.openssl.org/news/secadv/20170828.txt
https://www.openssl.org/news/secadv/20180327.txt

OpenSSL® is a registered trademark owned by the OpenSSL Software Foundation.

6 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].

7 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.

The OpenSSL development team has published an advisory concerning the OpenSSL vulnerabilities. Following the OpenSSL advisory, we found that CODESYS products are also affected.

8 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].

9 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/Advisory2018-06_CDS-53155.pdf

Change History

Version	Description	Date
1.0	First version	12.06.2018
2.0	Software update available	09.07.2018