



CODESYS

Advisory 2018-03

Security update for CODESYS SVN - OpenSSL update

Published: 15 March 2018

Version: 2.0

Template: templ_tecdoc_en_V2.0.docx

File name: Advisory2018-03_SVN-632.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	3
3.3	Difficulty	3
3.4	Existence of exploit	3
4	Available software updates	3
5	Further References	4
6	Mitigation	4
7	Acknowledgments	4
8	Further Information	4
9	Disclaimer	4
	Bibliography	5
	Change History	5

1 Affected Products

CODESYS SVN is an add on providing an SVN version control client integrated into the CODESYS V3 IDE. All CODESYS SVN versions based on OpenSSL 1.0.2 are affected; this includes all recent versions from 4.0.2.0 prior to V4.2.0.0.

There's no analysis for older versions, as they're based on older OpenSSL branches which are not officially supported any more, and most probably affected by issues of higher severity.

2 Vulnerability overview

2.1 Type

Private key exposure

2.2 Management Summary

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

2.3 References

CVE: CVE-2017-3736, CVE-2017-3737, CVE-2017-3738 (for vulnerabilities in OpenSSL) [6]

CODESYS JIRA: SVN-632, SVN-633, SVN-634

2.4 Severity Rating

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

The CVSS v3.0 base score of 6.8 has been assigned. The CVSS vector string is (CVSS:3.0/AV:N/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:N). [7]

3 Vulnerability details

3.1 Detailed Description

CODESYS SVN is an add on providing an SVN version control client integrated into the CODESYS IDE. CODESYS SVN uses the OpenSSL cryptographic software library. This advisory addresses the update of OpenSSL to the latest version to fix 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 V4.2.0.0 of CODESYS SVN, which solves the noted vulnerability issues.

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

5 Further References

CODESYS SVN version V4.2.0.0 fixes also another more critical security issue. Please see advisory 2017-08 for more information.

OpenSSL Security Advisories:

<https://www.openssl.org/news/secadv/20171102.txt>

<https://www.openssl.org/news/secadv/20171207.txt>

OpenSSL® is a registered trademark of The OpenSSL Software Foundation, Inc.

6 Mitigation

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

But 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 firewalls to protect and separate network zones
- Use VPN (Virtual Private Networks) and similar mechanisms to secure connections across the internet
- Generally, we advise to work in a controlled corporate environment

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 SVN is 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-training/codesys-support.html>
- [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/Advisory2018-03_SVN-632.pdf

Change History

Version	Description	Date
1.0	First version	21.02.2018
2.0	Software update available	15.03.2018