Advisory 2017-02

CODESYS V3

Security update for CODESYS SVN - OpenSSL update

Published: April 25, 2017

Version: 4.0
Template: templ_tecdoc_en_V2.0.docx
File name: Advisory2017-02_SVN-505.docx

CONTENT

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 including up to V4.1.0.x.

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

Remote DoS

2.2 Management Summary

A malicious server can cause the CODESYS SVN client to crash.

2.3 References

CVE: CVE-2017-3731, CVE-2016-7055 (for vulnerabilities in OpenSSL) [6]

CODESYS JIRA: SVN-505

2.4 Severity Rating

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

The CVSS v3 base score of 5.9 has been assigned. The CVSS 3.0 vector string is (CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:N/A:H). [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.

CVE-2017-3731: Truncated packet could crash via OOB read
Severity: Medium
The effect of this vulnerability is that a malicious server could crash the client.

CVE-2016-7055: Montgomery multiplication may produce incorrect results
Severity: Low
Upstream severity is low, and according to the OpenSSL advisory, the default configuration is not vulnerable.

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 CODESYS SVN V4.1.1.0 to solve this vulnerability issue.

5 Further References

OpenSSL Security Advisory:
https://www.openssl.org/news/secadv/20170126.txt
(refers also to https://www.openssl.org/news/secadv/20161110.txt)

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

6 Mitigation

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

- Avoid to connect to unknown / untrusted SVN servers via http(s) protocol
- Connect via svn+ssh:// protocol, which is not affected by this issue

Generally, we advise to work in a controlled corporate environment, and use of VPN (Virtual Private Networks) and similar mechanisms to secure connections across the internet.
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 support@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 download 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
[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/2017/Advisory2017-02_SVN-505.pdf

Change History

Version	Description	Date
1.0	First version	23.02.2017
2.0	Management Summary corrected	28.02.2017
3.0	New planned release date for software update	20.03.2017
4.0	Software update available, formal rework	25.04.2017