Advisory 2016-02

CODESYS V3

Security update for CODESYS SVN - Apache Subversion update

Published: April 25, 2017

Version: 3.0
Template: templ_tecdoc_en_V2.0.docx
File name: Advisory2016-02_SVN-433.docx

CONTENT

1 Affected Products

CODESYS SVN is an add on providing an SVN version control client integrated into the CODESYS IDE.

In the default configuration, the versions V4.1.0.x are affected. Older versions which were manually configured in the configuration file to use the SERF http client are also affected.

2 Vulnerability overview

2.1 Type

Remote DoS

2.2 Management Summary

A malicious http(s) server, or in the case of unencrypted http connections, a man in the middle can cause the client to use up CPU and memory (and possibly crash).

2.3 References

CVE: CVE-2016-8734 (for vulnerability in Apache Subversion) [6]

CODESYS JIRA: SVN-433

2.4 Severity Rating

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

The CVSS v3 base score of 3.7 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:L). [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. A malicious http(s) server, or in the case of unencrypted http connections, a man in the middle can cause the client to use up CPU and memory (and possibly crash).

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 Mitigation

3S-Smart Software Solutions GmbH has identified the follwing mitigating factors for this vulnerability:
- To avoid the man in the middle attack, use encrypted connections (https or svn+ssh) with certificate validation.
- The users should avoid to connect to unknown / untrusted SVN servers via http(s) protocol.

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].

6 Further References

Apache Subversion advisory:
https://subversion.apache.org/security/CVE-2016-8734-advisory.txt

Apache® and Subversion® are registred trademarks of The Apache Software Foundation.

7 Acknowledgments

This issue was found in Apache Subversion and reported to the Apache Subversion project by Florian Weimer, Red Hat, Inc.

Following the Apache Subversion advisory, 3S-Smart Software Solutions GmbH 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/2016/Advisory2016-02_SVN-433.pdf

Change History

Version	Description	Date
1.0	First version	14.12.2016
2.0	New planned release date for software update	20.03.2017
3.0	Software update available, formal rework	25.04.2017