Advisory 2017-08

Security update for CODESYS SVN - Apache Subversion® update

Published: 15 March 2018

Version: 3.0
Template: templ_tecdoc_en_V2.0.docx
File name: Advisory2017-08_SVN-585.docx

CONTENT

1 Affected Products

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

All versions are affected.

2 Vulnerability overview

2.1 Type

Remote code execution

2.2 Management Summary

A maliciously constructed URL could cause CODESYS SVN to run an arbitrary command. Such a URL could be generated by a malicious server, by a malicious user committing to a honest server (to attack another user of that server's repositories), or by a proxy server, or included in a manipulated CODESYS project file or project archive.

2.3 References

CVE: CVE-2017-9800 (for vulnerability in Apache Subversion®) [6]

CODESYS JIRA: SVN-585

2.4 Severity Rating

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

The CVSS v3.0 base score of 9.9 has been assigned. The CVSS vector string is (CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:C/C:H/I:H/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 sometimes connects to SVN urls which were not directly entered by the user. This can happen at least in the following use cases:

- during operations like 'checkout', 'update', and 'switch', when the tree being downloaded contains svn:externals properties.
- via the background monitoring (check for updates and locks) after the user opened a malicious CODESYS project (or project archive).
- when online operations like 'compare' or 'show log' are executed on a malicious project.
- automatic lock revalidation when switching from 'offline mode' to 'online mode' on a malicious project.

A maliciously constructed `svn+ssh://` URL would cause Subversion clients to run an arbitrary command. Such a URL could be generated by a malicious server, by a malicious user committing to a honest server (to attack another user of that server's repositories), or by a proxy server, or included in a manipulated CODESYS project file or project archive.

The vulnerability affects all clients, including those that use `file://`, `http://`, and plain (untunneled) `svn://`, as affected projects can contain 'svn:externals' properties using different URL schemes than the protocol used to access the project.

3.2 Exploitability

This vulnerability could be exploited remotely.

3.3 Difficulty

An attacker with low skills would be able to exploit this vulnerability.

3.4 Existence of exploit

According to the SVN security advisory, an exploit has been tested against standard SVN. We are not aware of any attacks specifically targeting CODESYS SVN.

4 Available software updates

3S-Smart Software Solutions GmbH has released versions V4.1.2.1 and V4.2.0.0 of CODESYS SVN, which solve the noted vulnerability issue.

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

5 Further References

Apache Subversion® advisory: [9]

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

6 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, or servers with untrusted users, or through untrusted proxy servers.
- The users should avoid to open CODESYS project files or project archives from untrusted sources.
- Server administrators may wish to review existing 'svn:externals' properties and install a 'pre-commit' hook that rejects commits that add invalid `svn+*://` URLs, in order to protect their users from other (malicious) users committing such URLs.

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.

This issue was discovered in Apache Subversion® by Joern Schneeweisz of Recurity Labs, and reported to the Apache Subversion® project by Jonathan Nieder.

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 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
[9] Apache Subversion® advisory: https://subversion.apache.org/security/CVE-2017-9800-advisory.txt

The latest version of this document can be found here:

https://customers.codesys.com/fileadmin/data/customers/security/2017/Advisory2017-08_SVN-585.pdf

Change History

Version	Description	Date
1.0	First version	11.08.2017
2.0	Software update available; typos corrected	28.09.2017
3.0	Further software update available	15.03.2018