Advisory 2017-09

Security update for CODESYS V3 web server

Published: December 20, 2017

Version: 2.0
Template: templ_tecdoc_en_V2.0.docx
File name: Advisory2017-09_CDS-57676.docx

CONTENT

1 Affected Products

In CODESYS V3 the web server is an optional part of the CODESYS runtime system. Therefore all CODESYS V3 runtime systems containing the web server in all versions prior V3.5.12.0 are affected, regardless of the CPU type or operating system:

- CODESYS Control V3 Runtime System Toolkit
- 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)
- CODESYS HMI V3

Versions of these products since V3.5.3.0 are typically affected only if an application on the device is using the CODESYS WebVisu because otherwise the web server is not active at all. Older versions are always affected.

2 Vulnerability overview

2.1 Type

Remote DoS

2.2 Management Summary

A crafted http or https request may lead to a complete loss of the webserver communication or may shut down the CODESYS runtime system completely.

2.3 References

CODESYS JIRA: CDS-57676, CDS-57679, CDS-57680, CDS-57681

2.4 Severity Rating

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

The CVSS v3.0 base score of 8.6 has been assigned. The CVSS vector string is (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:C/C:N/I:N/A:H). [7]

3 Vulnerability details

3.1 Detailed Description

The CODESYS web server is used by the CODESYS WebVisu to display CODESYS visualization screens in a web browser. A crafted http or https request may lead to a complete loss of the webserver communication or may shut down the CODESYS runtime system completely. Accordingly the web server will not be available for web browser requests anymore and will end up in a denial-of-service condition. Additionally, if the request has triggered the CODESYS runtime to shut down, the runtime stops executing the control application(s) and also all communication on other paths.

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

No known public exploits specifically target this vulnerability.

4 Available software updates

3S-Smart Software Solutions GmbH has released version V3.5.12.0, which solves the noted vulnerability issue for all affected CODESYS products.

This issue will also be fixed by V3.5.11.50 of the affected products, which is expected for mid of February 2018.

5 Mitigation

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
- Protect both development and control system from unauthorized access e. g. by means of the operating system
- 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].

6 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 vulnerability was reported internally by the CODESYS Security Team.

7 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].

8 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/2017/Advisory2017-09_CDS-57676.pdf

Change History

Version	Description	Date
1.0	First version	05.12.2017
2.0	Software update available	20.12.2017