Advisory 2019-11

Security update for CODESYS Control V2

Published: 18 December 2019

Version: 2.0
Template: templ_tecdoc_en_V2.0.docx
File name: Advisory2019-11_LCDS-325.docx

CONTENT

1 Affected Products

The following CODESYS V2 runtime systems are affected, regardless of the CPU type or operating system:

- CODESYS SP Realtime NT prior version V2.3.7.28
- CODESYS Runtime Toolkit 32 bit full prior version V2.4.7.54
- CODESYS PLCWinNT prior version V2.4.7.54

2 Vulnerability overview

2.1 Type

Null pointer dereference, remote DoS

2.2 Management Summary

A crafted request may cause a null pointer dereference in the affected CODESYS products which results in a denial-of-service condition.

2.3 References

CVE: CVE-2019-19789 [6]

CODESYS JIRA: LCDS-325, LCDS-327

2.4 Severity Rating

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

The CVSS v3.0 base score of 6.5 has been assigned. The CVSS vector string is (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H). [7]

3 Vulnerability details

3.1 Detailed Description

The CODESYS Control runtime system enables embedded or PC-based devices to be a programmable industrial controller. They provide communication servers for the communication with clients like the CODESYS Development System. A crafted request sent to this server may cause a null pointer dereference in the affected CODESYS products which results in a denial-of-service condition. The crafted request is only processed on the controller, if no online password is configured on the controller or if the attacker has previously successfully authenticated himself at the controller.

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 the following versions to solve the noted vulnerability issue for all affected CODESYS products:

• CODESYS SP Realtime NT version V2.3.7.28
• CODESYS Runtime Toolkit 32 bit full version V2.4.7.54
• CODESYS PLCWinNT version V2.4.7.54. This is also be part of the CODESYS Development System setup version V2.3.9.62.

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

5 Mitigation

3S-Smart Software Solutions GmbH recommends using the available software update to fix the vulnerability.

Password protection should be activated on the controllers whenever possible. If the patch could not be applied, the password protection also prevents the simple exploitation of this vulnerability, since in that case the CODESYS Control runtime system requires a successful authentication before the execution of the received services and does not execute a (crafted) service without login.

As part of a security strategy, 3S-Smart Software Solutions GmbH recommends the following general defense measures to reduce the risk of exploits:

• 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
• Activate and apply user management and password features
• Limit the access to both development and control system by physical means, operating system features, etc.
• 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.

We thank Chen Jie from NSFOCUS for reporting this vulnerability following coordinated disclosure.

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
[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/2019/Advisory2019-11_LCDS-325.pdf

Change History

Version	Description	Date
1.0	First version	05.12.2019
2.0	Software update available, CVE added, mitigation and security rating updated	18.12.2019