Advisory 2019-02

Security update for CODESYS Gateway V3 channel management

Published: 18 April 2019

Version: 2.0
Template: templ_tecdoc_en_V2.0.docx
File name: Advisory2019-02_CDS-65123.docx

CONTENT

1 Affected Products

All variants of the following CODESYS V3 products in all versions prior V3.5.14.20 containing the CmpGateway component are affected, regardless of the CPU type or operating system:
• CODESYS Control for BeagleBone
• CODESYS Control for emPC-A/iMX6
• CODESYS Control for IOT2000
• CODESYS Control for Linux
• CODESYS Control for PFC100
• CODESYS Control for PFC200
• CODESYS Control for Raspberry Pi
• CODESYS Control V3 Runtime System Toolkit
• CODESYS Gateway V3
• CODESYS V3 Development System

2 Vulnerability overview

2.1 Type

Use of Insufficiently Random Values, Unverified Ownership

2.2 Management Summary

The CODESYS Gateway - standalone or part of the affected products - does not correctly verify the ownership of a communication channel. The successful exploitation of this vulnerability may allow an attacker to close existing communication channels or to take over an already established user session to send crafted packets to a PLC.

2.3 References

CVE: CVE-2019-9010 [6]

CODESYS JIRA: CDS-65123, CDS-65124, CDS-65655, CDS-65656

2.4 Severity Rating

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

The CVSS v3.0 base score of 9.0 has been assigned. The CVSS vector string is (CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:C/C:H/I:H/A:H). [7]

3 Vulnerability details

3.1 Detailed Description

The CODESYS Gateway routes the online communication between clients like the CODESYS Development System and CODESYS Control runtime systems. As optional component of CODESYS Control runtime systems the CmpGateway may also run on PLC devices.

The CODESYS Gateway does not use adequate random values to identify the communication channel and insufficiently verifies the ownership of a channel. Successful exploitation of this vulnerability may allow an attacker to close existing communication channels. If the channel was not secured by encrypted communication, an attacker may also send crafted packages to a PLC within an already established user session.

3.2 Exploitability

This vulnerability could be exploited remotely.

3.3 Difficulty

An attacker with medium 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 V3.5.14.20, which solves the noted vulnerability issue for all affected CODESYS products.

This issue will also be fixed by version V3.5.15.0 of the affected products.
The release of version V3.5.15.0 is expected for July 2019.

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

5 Further References

See also Advisory 2019-03 for another CODESYS Gateway vulnerability.

6 Mitigation

Whenever possible the online communication to a CODESYS Control runtime system should be encrypted to prevent an attacker from taking over the channel. Depending on the PLC runtime system, these features can be activated by the user or only by the control manufacturer. Further information on how to activate encrypted communication and user management can be found in the CODESYS online help.

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:

- Conduct or reinforce security awareness training for users
- 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].

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.

We thank Martin Hartmann from cirosec GmbH for reporting this vulnerability following coordinated disclosure.

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
[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/Advisory2019-02_CDS-65123.pdf

Change History

Version	Description	Date
1.0	First version	09.04.2019
2.0	Software update available	18.04.2019