Advisory 2019-04

Security update for CODESYS Control V3 online user management

Published: 18 December 2019

CONTENT

1 Affected Products

All CODESYS Control V3 runtime systems prior version V3.5.13.0 containing the CmpUserMgr 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 PFC100
• CODESYS Control for PFC200
• CODESYS Control for Raspberry Pi
• CODESYS Control RTE V3
• CODESYS Control RTE V3 (for Beckhoff CX)
• CODESYS Control Win V3 (also part of the CODESYS Development System setup)
• CODESYS V3 Simulation Runtime (part of the CODESYS Development System)
• CODESYS Control V3 Runtime System Toolkit
• CODESYS HMI V3

2 Vulnerability overview

2.1 Type

Incorrect inherited permissions

2.2 Management Summary

The online user management of the CODESYS Runtime System may incorrectly grant access to sub objects, even if the logged-in user does not have inherited permission to access them.

2.3 References

CVE: CVE-2019-9008 [6]

ICS-CERT: ICSA-19-255-03 [8]

CODESYS JIRA: CDS-65847, CDS-58163

2.4 Severity Rating

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

The CVSS v3.0 base score of 8.8 has been assigned. The CVSS vector string is (CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H). [7]

3 Vulnerability details

3.1 Detailed Description

The CODESYS Runtime System enables embedded or PC-based devices to be a programmable industrial controller. For the communication with the CODESYS Development System or other clients, the implemented CODESYS protocol provides also access to directories, files, applications, symbols and so on. The online user management of the runtime system CODESYS Control controls access to all these objects. Sub objects such as a subdirectory inherit the access rights from the superordinate objects, if they have not been assigned their own access rights. The online user management may incorrectly grant access to such sub objects, even if the logged-in user does not have inherited permission to access them.

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 V3.5.13.0, which solves the noted vulnerability issue for all affected CODESYS products.

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 users to apply the available software updates.

Currently, 3S-Smart Software Solutions GmbH has not identified any workarounds for this vulnerability, in case the software update is not applied.

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
• 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 Martin Hartmann from cirosec GmbH 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.

Template: templ_tecdoc_en_V2.0.docx

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/Advisory2019-04_CDS-65847.pdf

Change History

Version	Description	Date
1.0	First version	22.07.2019
2.0	Public reference added	18.12.2019

Template: templ_tecdoc_en_V2.0.docx