Advisory 2017-05

Security update for HMAC signature check in CODESYS Control V3

Published: July 13, 2017

Version: 2.0
Template: templ_tecdoc_en_V2.0.docx
File name: Advisory2017-05_CDS-54476.docx

CONTENT

1 Affected Products

All CODESYS Control V3 Runtime Systems containing the CmpOpenSSL component prior version V3.5.11.0 are affected. The concerned function was initially released with version V3.5.8.0. For some of the products the CmpOpenSSL runtime system component was added in later versions than V3.5.8.0:

- CODESYS Control V3 Runtime System Toolkit
- CODESYS Control for BeagleBone (CmpOpenSSL included since V3.5.10.0)
- CODESYS Control for emPC-A/iMX6 (CmpOpenSSL included since V3.5.10.0)
- CODESYS Control for PFC200 (CmpOpenSSL included since V3.5.10.0)
- CODESYS Control for Raspberry Pi (CmpOpenSSL included since V3.5.10.0)
- CODESYS Control Win (all variants)

2 Vulnerability overview

2.1 Type

Return of wrong result code

2.2 Management Summary

The cryptographic function CryptoHMACVerify() provided by the CODESYS Control Runtime System to be used by OEM and end user implementations returns the result code ERR_OK (means HMAC is valid), even if the received HMAC signature does not match to the data.

Note: The security rating was estimated for typical use cases of the affected function in secure communication protocols. The real severity for a specific usage has to be investigated for each case separately.

2.3 References

CODESYS JIRA: CDS-54476, CDS-54501

2.4 Severity Rating

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

The CVSS v3 base score of 7.5 has been assigned. The CVSS 3.0 vector string is (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:H/A:N). [7]

3 Vulnerability details

3.1 Detailed Description

The function CryptoHMACVerify() is implemented by the CODESYS Control Runtime System component CmpOpenSSL. It can be called by OEM implementations referencing the CmpCryptoItf of the runtime system or by CODESYS applications using the CmpCrypto.library to check, if a received hashed message authentication code (HMAC) is valid or not. The function CryptoHMACVerify() returns the result code ERR_OK (means HMAC is valid), even if the received HMAC signature does not match to the data. In fact this means, CryptoHMACVerify() does not detect signature (HMAC) mismatches.

If the function CryptoHMACVerify() is not called by OEM or end user application or library code, the CODESYS Control Runtime System including its encrypted communication is not vulnerable by this issue.

3.2 Exploitability

Depends on the usage of CryptoHMACVerify() by the customer code.

3.3 Difficulty

Depends on the usage of CryptoHMACVerify() by the customer code.

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 V3.5.11.0, which solves the noted vulnerability issue for all affected CODESYS products [3].

For the following products 3S-Smart Software Solutions GmbH provides the fix also in patch version V3.5.10.50:

• CODESYS Control V3 Runtime System Toolkit

• CODESYS Control Win (all variants)

5 Mitigation

3S-Smart Software Solutions GmbH has not identified any workarounds for this vulnerability.

But 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 support@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 download 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
[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/Advisory2017-05_CDS-54476.pdf

Change History

Version	Description	Date
1.0	First version	30.05.2017
2.0	Software update available	13.07.2017