Advisory 2018-09

Security update for CODESYS Development System V3 Alarm configuration

Published: 23 October 2018

Version: 2.0
Template: templ_tecdoc_en_V2.0.docx
File name: Advisory2018-09_CDS-62131.docx

CONTENT

1 Affected Products

The CODESYS Development System contains an integrated compiler to generate code for execution on the CODESYS Control runtime systems. The compiler versions from V3.5.13.0 and before V3.5.13.20 of the CODESYS Development System imply this vulnerability. The affected compiler versions were introduced by the versions from V3.5.13.0 to V3.5.13.20 of all variants of the CODESYS Development System.

2 Vulnerability overview

2.1 Type

DoS, remote DoS

2.2 Management Summary

Crafted communication packets may exploit a vulnerability to prevent further communication with CODESYS Control runtime systems, if an affected compiler version of the CODESYS development system was used to download a CODESYS project with Alarm configuration to the runtime system.

2.3 References

CODESYS JIRA: CDS-62131, CDS-62177

2.4 Severity Rating

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

The CVSS v3.0 base score of 7.7 has been assigned. The CVSS vector string is (CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:C/C:N/I:N/A:H). [7]

3 Vulnerability details

3.1 Detailed Description

The CODESYS Development System contains an integrated compiler to generate code for execution on the CODESYS Control runtime systems. An error within a CODESYS library released with CODESYS V3.5.13.0 can be exploited causing an endless loop in a communication task on a CODESYS Control runtime system that was programmed with an affected CODESYS Development System. This endless loop occurs in a task of low priority and therefore remote access to an affected device can be prevented but the functionality of the control application itself will usually not be affected. This issue concerns only CODESYS projects containing an Alarm configuration.

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 V3.5.13.20 of the CODESYS Development System to solve the noted vulnerability issue.

This issue will also be fixed by version V3.5.14.0 of the affected products.

The release of version V3.5.14.0 is expected for December 2018.

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

The fix will only be effective if the compiler version used in the CODESYS projects is updated to a version >= V3.5.13.20.

5 Mitigation

3S-Smart Software Solutions GmbH has identified the following workaround for this vulnerability:
Using a compiler version prior to V3.5.13.0 to compile the CODESYS project. This allows the compiler to attract library versions without the issue described above. Be careful when using older compiler versions as this may affect some new features or cause other problems.

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
- 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.

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
[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/2018/Advisory2018-09_CDS-62131.pdf

Change History

Version	Description	Date
1.0	First version	11.10.2018
2.0	Software update available	23.10.2018