Advisory 2018-02

Security update for CODESYS Control V3 OPC UA Server

Published: 11 July 2018

Version: 4.0
Template: templ_tecdoc_en_V2.0.docx
File name: Advisory2018-02_CDS-58208.docx

CONTENT

1 Affected Products

All CODESYS Control V3 runtime systems prior version V3.5.13.0 containing both the OPC UA Server and the component CmpMemGC are affected. Runtime systems running only one of these two components are not affected by this vulnerability. The CODESYS OPC UA Server was initially released with version V3.5.6.20 of the CODESYS Control V3 runtime system.

Beside the CODESYS Control V3 Runtime System Toolkit, the following products are concerned by this issue:

• CODESYS Control RTE (all variants)

• CODESYS Control Win (all variants)

• CODESYS Control for BeagleBone prior to V3.5.9.20

• CODESYS Control for Raspberry Pi prior to V3.5.9.20

The above mentioned versions of CODESYS Control for BeagleBone and CODESYS Control for Raspberry Pi are only affected, if the CmpMemGC was explicitly activated within the CODESYSControl.cfg configuration file.

2 Vulnerability overview

2.1 Type

Heap based out-of-bounds write, remote DoS

2.2 Management Summary

A set of specific OPC UA requests may cause a write operation with an out of bounds write. As a result an access violation can occur and the CODESYS OPC UA Server ends up in a denial-of-service condition.

2.3 References

CODESYS JIRA: CDS-58208, CDS-58571, CDS-58572

2.4 Severity Rating

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

The CVSS v3.0 base score of 9.3 has been assigned. The CVSS vector string is (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:C/C:N/I:L/A:H). [7]

3 Vulnerability details

3.1 Detailed Description

The CODESYS OPC UA Server is an optional part of the CODESYS runtime system. The CODESYS OPC UA Server is used to exchange data between the runtime system and OPC UA clients like SCADA or HMIs.

A set of specific OPC UA requests may cause a write operation with an out-of-bounds write. Most likely as a result an access violation in the CODESYS OPC UA Server will occur and it may end up in a denial-of-service condition. Depending on the actual heap usage also heap memory of other parts of the CODESYS runtime system may be overwritten. The consequences in these cases are unclear.

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 versions V3.5.11.50, V3.5.12.10 and V3.5.13.0, which solve 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

To be vulnerable the CODESYS Control V3 runtime must contain both the OPC UA Server and the component CmpMemGC. As the CmpMemGC is an optional component, it can be removed from configuration, if its memory book keeping functionality is not needed. For statically linked runtime systems this means a recompile of the runtime system code. However if the CmpMemGC is dynamically loaded, it can be deactivated in the runtime system configuration file CODESYSControl.cfg.

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
- 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/Advisory2018-02_CDS-58208.pdf

Change History

Version	Description	Date
1.0	First version	06.02.2018
2.0	Software update available	14.02.2018
3.0	Further software update available, affected products specified more precisely	26.02.2018
4.0	Further software update available, link to support contact site adapted	09.07.2018