



CODESYS

Advisory 2018-01

Security update for CODESYS V2.3 web server

Published: February 2nd, 2018

Version: 3.0

Template: templ_tecdoc_en_V2.0.docx

File name: Advisory2018-01_LCDS-282.docx

CONTENT

	Page	
1	Affected Products	3
2	Vulnerability overview	3
2.1	Type	3
2.2	Management Summary	3
2.3	References	3
2.4	Severity Rating	3
3	Vulnerability details	3
3.1	Detailed Description	3
3.2	Exploitability	3
3.3	Difficulty	3
3.4	Existence of exploit	3
4	Available software updates	3
5	Mitigation	4
6	Acknowledgments	4
7	Further Information	4
8	Disclaimer	4
	Bibliography	5
	Change History	5

1 Affected Products

All Microsoft Windows (also WinCE) based CODESYS V2.3 web servers running stand-alone or as part of the CODESYS runtime system prior version V1.1.9.19 are affected.

2 Vulnerability overview

2.1 Type

Stack overflow and remote code execution

2.2 Management Summary

A crafted request may cause a buffer overflow and could therefore execute arbitrary code on the web server or lead to a denial-of-service condition due to a crash in the web server.

2.3 References

CVE: CVE-2018-5440 [6]

ICS-CERT: ICS-CERT: ICSA-18-032-02 [8]

CODESYS JIRA: LCDS-282, LCDS-283

2.4 Severity Rating

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

The CVSS v3.0 base score of 9.8 has been assigned. The CVSS vector string is CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H). [7]

3 Vulnerability details

3.1 Detailed Description

The CODESYS web server is used by the CODESYS WebVisu to visualize CODESYS screens in a web browser. A crafted web server request may cause a buffer overflow and could therefore execute arbitrary code on the web server or lead to a denial-of-service condition due to a crash in the web server.

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 the CODESYS web server V.1.1.9.19 for CODESYS V2.3 to solve this vulnerability issue. This is also part of the CODESYS setup V2.3.9.56.

Note: Only for web servers of version V1.1.9.18 running on devices of the WinCE ARM architecture: This update will also correct the bug fix for LCDS-252 (Advisory 2016-01), as the original fix could cause a sporadic misalignment exception during normal operation on these devices.

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

5 Mitigation

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

We thank Zhu WenZhe of Istury IOT security lab. 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.

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-training/codesys-support.html>
- [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/Advisory2018-01_LCDS-282.pdf

Change History

Version	Description	Date
1.0	First version	23.01.2018
2.0	Software update available	30.01.2018
3.0	CVE and ICSA reference numbers added	02.02.2018