Advisory 2016-01

CODESYS V2.3

Security update for CODESYS V2.3 web server

Published: April 25, 2017

Version: 3.0
Template: templ_tecdoc_en_V2.0.docx
File name: Advisory2016-01_LCDS-252.docx

CONTENT

1 Affected Products

All CODESYS V2.3 web servers running stand-alone or as part of the CODESYS runtime system prior version V1.1.9.18 are affected. The CODESYS V3 web server is unconcerned by this vulnerability.

2 Vulnerability overview

2.1 Type

Arbitrary file upload, buffer overflow, remote DoS

2.2 Management Summary

A crafted request may allow to upload arbitrary files to the CODESYS web server without authorization. Further on a buffer overflow could crash this web server and lead to a denial-of-service condition.

2.3 References

ICS-CERT: ICS-VU-633864, Advisory: ICSA-17-087-02 [8]

CVE: CVE-2017-6025 and CVE-2017-6027 [6]

CODESYS JIRA: LCDS-252

2.4 Severity Rating

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

The CVSS v3 base score of 9.8 has been assigned. The CVSS 3.0 vector string is (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 allow to upload arbitrary files to the CODESYS web server without authorization. Further on a buffer overflow in this area could crash the web server and lead to a denial-of-service condition.

3.2 Exploitability

This vulnerability could be exploited remotely.

3.3 Difficulty

An attacker with medium 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.1.1.9.18 for CODESYS V2.3 to solve this vulnerability issue.

The default restriction for recipe files is now a maximum file size of 50000 bytes per recipe file and a maximum number of 20 recipe files.

With the following parameters the maximum recipe file size and the maximum number of recipe files can be configured in the webserver_conf.xml file.
<max-recipe-file-size> 50000 </max-recipe-file-size>
<max-recipe-files> 20 </max-recipe-files>

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

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 David Atch of CyberX 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 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/2016/Advisory2016-01_LCDS-252.pdf

Change History

Version	Description	Date
1.0	First version	16.11.2016
2.0	Software update available	30.11.2016
3.0	Security rating updated, further ICS-CERT and CVE references added, formal rework	25.04.2017