Advisory 2021-05

Security update for CODESYS Automation Server

Published: 28 April 2020

Version: 1.0
Template: templ_tecdoc_en_V3.0.docx
File name: Advisory2021-05_CAS-2238.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

CODESYS Automation Server versions before V1.16.0 are affected. CODESYS GmbH has already updated all instances to this fix version.

2 Vulnerability overview

2.1 Type

CWE-352: Cross-Site Request Forgery (CSRF) [7]

2.2 Management Summary

Manipulated files of a CODESYS Web Visualization deployed on a controller can lead to a privilege escalation when the Web Visualization is opened with the CODESYS Automation Server.

2.3 References

CVE: CVE-2021-29238 [6]

CODESYS JIRA: CAS-2238

2.4 Severity Rating

CODESYS GmbH has rated this vulnerability as high.

The CVSS v3.0 base score of 8.0 has been assigned. The CVSS vector string is (CVSS:3.0/AV:N/AC:H/PR:L/UI:R/S:C/C:H/I:H/A:H). [8]

3 Vulnerability details

3.1 Detailed Description

The CODESYS Automation Server supports the display of CODESYS Web Visualization via a secure connection. Manipulated CODESYS Web Visualization files can lead to privilege escalation, since malicious JavaScript code in the manipulated files can send https requests to the CODESYS Automation Server with the permissions of the user viewing the Web Visualization.

3.2 Exploitability

This vulnerability could be exploited remotely. As precondition, an attacker needs to either manipulate the application files before they are deployed on a controller connected to the CODESYS Automation Server, or have write access to the controllers file system directly.

3.3 Difficulty

An attacker with high 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

CODESYS GmbH has already updated all CODESYS Automation Server instances to V1.16.0. No further software updates are needed to fix this vulnerability.

5 Mitigation

CODESYS GmbH has already updated all CODESYS Automation Server instances to this fix version. Furthermore, we have not found any indication that in any way indicate the exploitation of the vulnerability.

As a general rule of precaution, the user accounts created in the CODESYS Automation Server should always be created with the minimal amount of permissions the user needs to perform their job. Administrator accounts should only be used for administrative purposes; administrative users can create a secondary account with restricted permissions to perform their non-administrative work.

Furthermore, CODESYS GmbH strongly recommends using the two-factor authentication of the CODESYS Automation server to also prevent similar attacks.

6 Acknowledgments

This issue was discovered by Uri Katz of Claroty.

CODESYS GmbH thanks for reporting following coordinated disclosure. This helps us to improve our products and to protect customers and users.

7 Further Information

For additional information regarding the CODESYS products, especially the above-mentioned versions, or about the described vulnerability please contact the CODESYS support team [5].

8 Disclaimer

CODESYS 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 CODESYS GmbH. Insofar as permissible by law, however, none of this information shall establish any guarantee, commitment or liability on the part of CODESYS GmbH.

Note: Not all CODESYS features are available in all territories. For more information on geographic restrictions, please contact sales@codesys.com.

Bibliography

[1] CODESYS GmbH: CODESYS Security Whitepaper
[2] CODESYS GmbH: Coordinated Disclosure Policy
[3] CODESYS GmbH update area: https://www.codesys.com/download
[4] CODESYS GmbH security information page: https://www.codesys.com/security
[5] CODESYS GmbH support contact site: https://www.codesys.com/support
[6] Common Vulnerabilities and Exposures (CVE): https://cve.mitre.org
[7] Common Weakness Enumeration (CWE): https://cwe.mitre.org
[8] CVSS Calculator: https://www.first.org/cvss/calculator/3.0
[9] ICS-CERT: https://ics-cert.us-cert.gov

The latest version of this document can be found here:

https://customers.codesys.com/index.php?eID=dumpFile&t=f&f=14638&token=30b75ee95d0d94527894dfd8cdc5432575a8eff8&download=

Change History

Version	Description	Date
1.0	First version	28.04.2021