Advisory 2021-07

Security update for CODESYS V2 web server

Published: 15 July 2021

Version: 4.0
Template: templ_tecdoc_en_V3.0.docx
File name: Advisory2021-07_LCDS-339.docx

CONTENT

1 Affected Products

All CODESYS V2 web servers running stand-alone or as part of the CODESYS runtime system prior version V1.1.9.20 are affected.

2 Vulnerability overview

2.1 Type

Multiple, see description. [7]

2.2 Management Summary

Crafted web server requests may read or write arbitrary memory or files in the CODESYS Control runtime system or may cause invalid memory accesses to execute code or to crash the CODESYS web server or the CODESYS Control runtime system.

2.3 References

CVE: CVE-2021-30189, CVE-2021-30190, CVE-2021-30191, CVE-2021-30192, CVE-2021-30193, CVE-2021-30194 [6]

CODESYS JIRA: LCDS-339, LCDS-344

2.4 Severity Rating

CODESYS GmbH has rated this vulnerability as critical.

The CVSS v3.0 base score of 10 has been assigned. The CVSS vector string is (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H). [8]

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. It has the following vulnerabilities:

CVE-2021-30189: CWE-121: Stack-based Buffer Overflow
Crafted web server requests may cause a stack-based buffer overflow and could therefore execute arbitrary code on the CODESYS web server or trigger a denial-of-service condition due to a crash in the CODESYS web server.

CVE-2021-30190: CWE-284: Improper Access Control
The user management of the CODESYS V2.3 WebVisu allows user-dependent control of access to the visualization pages. However, subordinate requests to read or write values are forwarded to the CODESYS Control runtime system regardless of successful authentication. This enables crafted web server requests to bypass the user management and to read or write values on the PLC without authentication.

CVE-2021-30191: CWE-120: Buffer Copy without Checking Size of Input
Crafted web server requests can cause an over-read or over-write of a buffer in the CODESYS web server, which usually leads to a denial-of-service condition.

CVE-2021-30192: CWE-358: Improperly Implemented Security Check
Crafted web server requests can bypass the security checks for boot project-related files on the CODESYS Control runtime system to upload them from the CODESYS Control runtime system.

CVE-2021-30193: CWE-787: Out-of-bounds Write
Crafted web server requests can be utilized to write arbitrary memory in the CODESYS Control runtime system and could therefore execute code on the CODESYS Control runtime system or lead to a denial-of-service condition due to a crash of the CODESYS Control runtime system.

CVE-2021-30194: CWE-125: Out-of-bounds Read
Crafted web server requests can be utilized to read arbitrary memory in the CODESYS Control runtime system or can also crash the CODESYS web server.

3.2 Exploitability

These vulnerabilities could be exploited remotely.

3.3 Difficulty

An attacker with low skills would be able to exploit these vulnerabilities.

3.4 Existence of exploit

No known public exploits specifically target these vulnerabilities.

4 Available software updates

CODESYS GmbH has released version V1.1.9.20 of the CODESYS V2 web server to solve the noted vulnerability issues. This version of the CODESYS V2 web server is also part of the CODESYS Development System setup version V2.3.9.66.

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

Update:
For compatibility reasons, starting from version V1.1.9.21 the CODESYS web server supports the new setting disable-secure-monitoring in webserver_conf.xml. This setting re-enables direct monitoring of var_inout variables of function blocks in addition to the usual monitoring of the caller variables. Since this setting weakens the security checks introduced to prevent CVE-2021-30194 attacks, CODESYS GmbH strongly recommends enabling this setting only if this feature is really needed by a specific CODESYS Webvisu application. Furthermore, enabling this setting requires a secure environment or appropriate compensation means.

CODESYS GmbH has released version V1.1.9.21 of the CODESYS V2 web server both stand-alone and also as part of the CODESYS Development System setup version V2.3.9.67.

5 Mitigation

CODESYS GmbH recommends using the available software update to fix the vulnerabilities.

Currently, CODESYS GmbH has not identified any specific workarounds for these vulnerabilities, in case the software update is not applied.

As part of a security strategy, CODESYS GmbH recommends the following general defense measures to reduce the risk of exploits:
• 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
• Use encrypted communication links
• 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

CVE-2021-30189, CVE-2021-30194:
These issues were discovered by Vyacheslav Moskvin, Sergey Fedonin and Anton Dorfman of Positive Technologies.

CVE-2021-30190, CVE-2021-30191, CVE-2021-30192, CVE-2021-30193:
These issues were discovered by Vyacheslav Moskvin and Anton Dorfman of Positive Technologies.

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=14726&token=553da5d11234bbe1ceed59969d419a71bb8c8747&download=

Change History

Version	Description	Date
1.0	First version	28.04.2021
2.0	Software update available	11.05.2021
3.0	Available software updates: Compatibility notes added	29.06.2021
4.0	Further software update available	15.07.2021