Advisory 2021-15

Security update for CODESYS V2 web server

Published: 08 November 2021

Version: 3.0
Template: templ_tecdoc_en_V3.0.docx
File name: Advisory2021-15_LCDS-358.docx

CONTENT

1 Affected Products

All CODESYS V2 web servers running stand-alone or as part of the CODESYS runtime system prior version V1.1.9.22 are affected.

2 Vulnerability overview

2.1 Type

Multiple, see description. [7]

2.2 Management Summary

Crafted web server requests may cause invalid memory accesses to crash the CODESYS web server or may read stack or heap memory.

2.3 References

CVE: CVE-2021-34583, CVE-2021-34584, CVE-2021-34585, CVE-2021-34586 [6]

CODESYS JIRA: LCDS-358, LCDS-360

2.4 Severity Rating

CODESYS GmbH has rated this vulnerability as high.

The CVSS v3.0 base score of 8.2 has been assigned. The CVSS vector string is (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/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. A remote attacker can exploit the following vulnerabilities:

CVE-2021-34583: CWE-122: Heap-based Buffer Overflow
CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H
Crafted web server requests may cause a heap-based buffer overflow and could therefore trigger a denial-of-service condition due to a crash in the CODESYS web server.

CVE-2021-34584: CWE-126: Buffer Over-read
CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:H
Crafted web server requests can be utilized to read partial stack or heap memory or may trigger a denial-of-service condition due to a crash in the CODESYS web server.

CVE-2021-34585: CWE-252: Unchecked Return Value
CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H
Crafted web server requests can trigger a parser error. Since the parser result is not checked under all conditions, a pointer dereference with an invalid address can occur. This leads to a denial of service situation in the CODESYS web server.

CVE-2021-34586: CWE-476: NULL Pointer Dereference
CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H
Crafted web server requests may cause a Null pointer dereference in the CODESYS web server and may result in a denial-of-service condition.

Since V1.1.9.20, the CODESYS web server only processes these manipulated requests, if the CODESYS V2.3 WebVisu user management is not activated or if the attacker has previously successfully authenticated himself on the CODESYS web server. The user management of earlier versions of the CODESYS web server does not protect against these attacks.

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

POC is publicly available.

4 Available software updates

CODESYS GmbH has released version V1.1.9.22 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 V2.3.9.68.

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

5 Mitigation

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

The user management of the CODESYS V2.3 WebVisu allows user-dependent control of access to the visualization pages. Since V1.1.9.20 of the CODESYS web server, activating the user management will also prevent the attacks described above, even in the case that 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

These vulnerabilities were discovered by Tenable Research.

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=16876&token=a3f1d937f95e7034879f4f2ea8e5a99b168256a7&download=

Change History

Version	Description	Date
1.0	First version	18.10.2021
2.0	Software update available	25.10.2021
3.0	POC is publicly available	08.11.2021