Advisory 2022-13

Security update for CODESYS Gateway V2

Published: 23 June 2022

Version: V2.0
Template: templ_tecdoc_en_V3.0.docx
File name: Advisory2022-13_LCDS-376.docx

CONTENT

1 Affected Products

All versions of the following CODESYS V2 product prior version V2.3.9.38 are affected:
• CODESYS Gateway Server

2 Vulnerability overview

2.1 Type

CWE-187: Partial String Comparison, CWE-400: Uncontrolled Resource Consumption, CWE-789: Memory Allocation with Excessive Size Value [7]

2.2 Management Summary

An unauthenticated attacker would be able to send crafted requests to cause the CODESYS Gateway Server V2 to allocate excessive memory or consume all available TCP client connections. Besides, passwords are insufficiently checked during login.

2.3 References

CVE: CVE-2022-31802, CVE-2022-31803, CVE-2022-31804 [6]

CODESYS JIRA: LCDS-376

2.4 Severity Rating

CODESYS GmbH has rated this vulnerability as critical.

The CVSS v3.1 base score of 9.8 has been assigned. The CVSS vector string is (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H). [8]

3 Vulnerability details

3.1 Detailed Description

The CODESYS Gateway routes the online communication between clients like the CODESYS Development System and CODESYS Control runtime systems. An unauthenticated attacker would be able to send crafted requests to exploit the following vulnerabilities:

CVE-2022-31802: CWE-187: Partial String Comparison:
CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H
The CODESYS Gateway Server V2 does not sufficiently verify the specified password during login. Therefore, an attacker could successfully perform authentication by specifying a shorter password than the configured one.

CVE-2022-31803: CWE-400: Uncontrolled Resource Consumption
CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:L
The CODESYS Gateway Server V2 insufficiently checks the activity of TCP client connections. This allows an unauthenticated attacker to consume all available TCP connections and prevent legitimate users or clients from establishing a new connection to the CODESYS Gateway Server V2. Existing connections are not affected and therefore remain intact.

CVE-2022-31804: CWE-789: Memory Allocation with Excessive Size Value
CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H
The CODESYS Gateway Server V2 allocates memory based on the content of the request but does not ensure that the size is within expected limits. Thus, an unauthenticated attacker could trigger the allocation of arbitrary amounts of memory, which could possibly lead to a crash of the Gateway due to an out-of-memory condition.

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 V2.3.9.38 of the CODESYS Gateway Server, which is also part of the CODESYS Development System setup version V2.3.9.69.

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

Compatibility note for CVE-2022-31802:
If clients previously used a short-form password, they must log in with the full password after the update to continue to authenticate successfully.

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-2022-31803, CVE-2022-31804: These issues were reported by Divya Suvarna of ABB Device Security Assurance Center.

CVE-2022-31802: This issue was reported internally by the CODESYS team.

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/3.1
[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=17141&token=17867e35cfd30c77ba0137f9a17b3a557a4b7b66&download=

Change History

Version	Description	Date
1.0	First version	09.06.2022
2.0	Software update available	23.06.2022