



CODESYS Gateway Client - Uncontrolled Memory Allocation

CODESYS Security Advisory 2026-11

Published: 2026-09-30

Last Change: 2026-09-30

Identifiers, Type and Severity

CVE-2026-76992

CERT@VDE: VDE-2026-094

CODESYS: CDS-98296, CDS-98387

CWE-770: Allocation of Resources Without Limits or Throttling

CVSS v3.1 Base Score: 7.5 | High | CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H

1 Summary

The CODESYS Gateway Client (CmpGatewayClient) is used by various CODESYS products to establish PLC communication via the CODESYS Gateway.

Due to missing limits on memory allocations derived from a size field in a gateway response, a malicious gateway can cause excessive memory consumption in the client, resulting in a denial-of-service condition.

The vulnerability can be exploited when an affected product connects to an attacker-controlled gateway.

2 Affected Products

The following products are affected in all versions from 3.0.0.0 and before 3.5.22.40.

- CODESYS Development System 3
- CODESYS Gateway
- CODESYS Edge Gateway for Windows
- CODESYS HMI (SL)
- CODESYS OPC DA Server SL
- CODESYS PLCHandler
- CODESYS Runtime Toolkit

The following products are affected in all versions from 3.5.15.0 and before 4.23.0.0.

- CODESYS Edge Gateway for Linux

3 Impact

Successful exploitation may result in excessive memory consumption, leading to a denial-of-service condition in the affected client.

4 Remediation

Update the following products to version 3.5.22.40.

- CODESYS Development System 3
- CODESYS Gateway
- CODESYS Edge Gateway for Windows
- CODESYS HMI (SL)
- CODESYS OPC DA Server SL
- CODESYS PLCHandler
- CODESYS Runtime Toolkit

Update the following product to version 4.23.0.0. The release of this version is expected in Q4 2026.

- CODESYS Edge Gateway for Linux

The CODESYS Development System and the products available as CODESYS add-ons can be downloaded and installed directly with the CODESYS Installer or be downloaded from the CODESYS Store. Alternatively, as well as for all other products, you will find further information on obtaining the software update in the CODESYS Update area <https://www.codesys.com/download/>.

5 General Security Recommendations

As part of a security strategy, CODESYS GmbH strongly recommends at least the following best-practice defense measures:

- 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

- Activate and apply user management and password features
- Limit the access to both development and control system by physical means, operating system features, etc.
- Use encrypted communication links
- Use VPN (Virtual Private Networks) tunnels if remote access is required
- 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](#).

6 Acknowledgments

Reported by Delta Electronics Inc.

Coordination done by CERT@VDE.

CODESYS GmbH thanks all parties involved for their efforts.

7 Further Information

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

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.

9 Bibliography

- [1] CERT@VDE: <https://cert.vde.com>
- [2] CODESYS GmbH: [CODESYS Security Whitepaper](#)
- [3] CODESYS GmbH: [Coordinated Disclosure Policy](#)
- [4] CODESYS GmbH download area: <https://www.codesys.com/download>
- [5] CODESYS GmbH security information page: <https://www.codesys.com/security>
- [6] CODESYS GmbH support contact site: <https://www.codesys.com/support>
- [7] Common Vulnerabilities and Exposures (CVE): <https://cve.mitre.org>
- [8] Common Weakness Enumeration (CWE): <https://cwe.mitre.org>
- [9] CVSS Calculator: <https://www.first.org/cvss/calculator/3.1>

The latest version of this document can be found here:

https://api-www.codesys.com/fileadmin/user_upload/CODESYS_Group/Ecosystem/Up-to-Date/Security/Security-Advisories/Advisory2026-11_CDS-98296.pdf

Change History

Version	Description	Date
1.0	Initial version	2026-09-30