



# CODESYS EtherNetIP - Improper timeout handling

CODESYS Security Advisory 2026-04

Published: 2026-04-23

Last Change: 2026-04-23

## Identifiers, Type and Severity

CVE-2026-35225

CERT@VDE: VDE-2026-040

CODESYS: EIP-1011

CWE-754: Improper Check for Unusual or Exceptional Conditions

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

CODESYS EtherNet/IP is an add-on for the CODESYS Development System that provides a fully integrated EtherNet/IP protocol stack along with diagnostic capabilities. A flaw in the EtherNet/IP adapter protocol stack library results in a vulnerability within the generated application code. When an EtherNet/IP adapter is configured, this vulnerable protocol stack is downloaded to and executed by CODESYS Control runtime systems.

Under certain non-standard operating conditions, the EtherNet/IP adapter fails to perform timeout checks on active TCP connections. As a result, once all available TCP connections are in use, expired connections are not released and no new TCP connections can be established. Existing connections remain unaffected and continue to operate normally.

This issue affects only CODESYS projects that include an EtherNet/IP adapter configuration.

## 2 Affected Products

The following product is affected in all versions before 4.9.0.0:

- CODESYS EtherNetIP

## 3 Impact

Exploitation of this vulnerability may allow an unauthenticated remote attacker to exhaust all available TCP connections in the CODESYS EtherNet/IP adapter stack running on a CODESYS Control runtime system, thereby preventing legitimate clients from establishing new connections.

## 4 Remediation

Update the following product to version 4.9.0.0.

- CODESYS EtherNetIP

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

This issue was reported by ABB.

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](mailto: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/Advisory2026-04\\_EIP-1011.pdf](https://api-www.codesys.com/fileadmin/user_upload/CODESYS_Group/Ecosystem/Up-to-Date/Security/Security-Advisories/Advisory2026-04_EIP-1011.pdf)

## Change History

Version	Description	Date
1.0	Initial version	2026-04-23