CODESYS Automation Server Connector and CODESYS Service Tool - multiple vulnerabilities

CODESYS Security Advisory 2026-13

Published: 2026-11-17

Last Change: 2026-11-17

Identifiers, Type and Severity

CVE-2026-118496, CVE-2026-118497

CERT@VDE: VDE-2026-145

CODESYS: CAS-5434, CAS-5435

CWE-706: Use of Incorrectly-Resolved Name or Reference,
CWE-295: Improper Certificate Validation

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

© CODESYS Group

1 Summary

The CODESYS Automation Server Connector is an Add-on for the CODESYS Development System that enables project synchronization with the CODESYS Automation Server and the configuration of CODESYS Edge Gateways. The CODESYS Service Tool is a stand-alone application for configuring CODESYS Edge Gateways.

Multiple vulnerabilities in the affected products could allow an unauthenticated remote attacker to manipulate trusted CODESYS Automation Server interactions. Successful exploitation may result in the interception and manipulation of Automation Server communications or arbitrary code execution with the privileges of the user running the affected product.

CVE-2026-118496:

CWE-706: Use of Incorrectly-Resolved Name or Reference

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

The affected products process a server-supplied URL without sufficient validation. An unauthenticated remote attacker controlling a malicious Automation Server and tricking a user to trust it, or performing a man-in-the-middle attack, can exploit this vulnerability by causing the affected product to process unintended content instead of the expected URL. Successful exploitation may result in arbitrary code execution with the privileges of the user running the affected product.

CVE-2026-118497:

CWE-295: Improper Certificate Validation

CVSS v3.1 Base Score: 6.8 | Medium | CVSS:3.1/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:N

The affected products do not sufficiently validate CODESYS Automation Server TLS certificates when a user starts the certificate enrollment. An unauthenticated remote attacker performing a man-in-the-middle attack can exploit this vulnerability by supplying an untrusted certificate that is accepted as trusted. Successful exploitation may allow an attacker to intercept and manipulate communications between the CODESYS Automation Server and the PLC network.

Template: templ_tecdoc_en_V3.0.docx

2 Affected Products

The following products are affected in all versions from 1.0.0.0 and before 1.40.0.0.
• CODESYS Automation Server Connector
• CODESYS Service Tool

3 Impact

Successful exploitation of these vulnerabilities may allow an unauthenticated remote attacker to intercept and manipulate Automation Server communications with the PLC network, or execute arbitrary code on the host running the affected products, resulting in a loss of confidentiality, integrity, and availability.

4 Remediation

Update the following products to version 1.40.0.0.
• CODESYS Automation Server Connector
• CODESYS Service Tool

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/.

© CODESYS Group

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 f0rw4rd aka Felix Eberstaller of Limes Security / QuellSec.

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.

Template: templ_tecdoc_en_V3.0.docx

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:

© CODESYS Group

https://api-www.codesys.com/fileadmin/user_upload/CODESYS_Group/Ecosystem/Up-to-Date/Security/Security-Advisories/Advisory2026-13_CAS-5434.pdf

Change History

Version	Description	Date
1.0	Initial version	2026-11-17

Template: templ_tecdoc_en_V3.0.docx

© CODESYS Group