CODESYS Automation Server Connector path traversal

CODESYS Security Advisory 2026-14

Published: 2026-11-17

Last Change: 2026-11-17

Identifiers, Type and Severity

CVE-2026-118498
CERT@VDE: VDE-2026-146
CODESYS: CAS-5436

CWE-22: Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')

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

© CODESYS Group

1 Summary

CODESYS Automation Server Connector is an Add-on for the CODESYS Development System to synchronize projects on the CODESYS Automation Server and to configure CODESYS Edge Gateways.

The CODESYS Automation Server Connector uses server-supplied file names without sufficient path traversal checks. An unauthenticated remote attacker controlling a malicious Automation Server, or performing a man-in-the-middle attack on a trusted communication channel, can exploit this vulnerability to perform arbitrary file writes outside the intended working directory of the affected products. Successful exploitation requires execution of commands via the affected scripting interface and may allow subsequent arbitrary code execution with the privileges of the user running the CODESYS Development System.

2 Affected Products

The following products are affected in all versions from 1.23.0.0 and before 1.40.0.0.

• CODESYS Automation Server Connector

3 Impact

Successful exploitation may allow an unauthenticated remote attacker to write attacker-controlled files to arbitrary locations on the engineering workstation. This may subsequently result in remote code execution with the privileges of the user running the CODESYS Development System.

4 Remediation

Update the following products to version 1.40.0.0.

• CODESYS Automation Server Connector

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.

Template: templ_tecdoc_en_V3.0.docx

© CODESYS Group

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.

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/Advisory2026-14_CAS-5436.pdf

Change History

Version	Description	Date
1.0	Initial version	2026-11-17

Template: templ_tecdoc_en_V3.0.docx

© CODESYS Group