CODESYS Development System - Incorrect Default Permissions

CODESYS Security Advisory 2026-09

Published: 2026-05-21

Last Change: 2026-05-21

Identifiers, Type and Severity

CVE-2026-44468, CVE-2026-44469

CERT@VDE: VDE-2026-055

CODESYS: CDS-97365, CDS-97423, CDS-97483, CDS-97484

CWE-276: Incorrect Default Permissions

CVSS v3.1 Base Score: 7.8 | High | CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H

1 Summary

Two local privilege escalation vulnerabilities were identified in the CODESYS Development System. Specifically, the PackageManager and the IPM create temporary directories with insecure default permissions when executed with administrative privileges. This allows low-privileged local users to modify a temporary bootstrap file to force the deployment of arbitrary components, or to exploit a Time-of-Check to Time-of-Use (TOCTOU) race condition to replace digitally verified installation files with malicious ones prior to installation. Both flaws bypass intended security boundaries during the installation of packages or add-ons.

2 Affected Products

The following product is affected in all versions before 3.5.22.20:
• CODESYS Development System

3 Impact

Successful exploitation of these two vulnerabilities allows a low-privileged local attacker to achieve local privilege escalation. Because the installation processes of the PackageManager and the IPM run with elevated administrative privileges, any manipulated bootstrap file will be applied or any installation file will be installed in this high-privilege context. This enables the attacker to install arbitrary files to compromise the underlying operating system.

4 Remediation

Update the following product to version 3.5.22.20.
• CODESYS Development System

The CODESYS Development System 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 David Ruscheweyh of SEW-EURODRIVE GmbH & Co KG.

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/Advisory2026-09_CDS-97365.pdf

Change History

Version	Description	Date
1.0	Initial version	2026-05-21