CODESYS Installer - Possible Privilege Escalation

CODESYS Security Advisory 2026-01

Published: 2026-03-10

Last Change: 2026-03-10

Identifiers, Type and Severity

CVE-2026-2364

CERT@VDE: VDE-2026-012

CODESYS: INST-1084, INST-1091

CWE-367: Time-of-check Time-of-use (TOCTOU) Race Condition

CVSS v3.1 Base Score: 7.3 | High | CVSS:3.1/AV:L/AC:L/PR:L/UI:R/S:U/C:H/I:H/A:H

1 Summary

The CODESYS Installer is affected by a privilege escalation vulnerability. Due to a race condition, a local attacker with limited privileges can replace the verified downloaded setup before execution. Because the update process runs with administrator privileges, a malicious application can be executed with elevated rights.

The attack requires the legitimate user to confirm the self-update prompt for the CODESYS Installer itself or to initiate an installation of a CODESYS Development System. The update process for CODESYS Add-Ons is not affected by this issue.

2 Affected Products

The following product is affected in all versions before 2.6.1.0.

• CODESYS Installer

3 Impact

Exploitation of this vulnerability can lead to a privilege escalation on the host system.

4 Remediation

Update the following product to version 2.6.1.0.

• CODESYS Installer

To avoid using the self-update mechanism when applying the software update, we recommend manually downloading the fixed version of the CODESYS Installer from the CODESYS Store and installing it. Alternatively, you can also download and install the CODESYS Development System version 3.5.22.0 or newer as a complete setup, which includes the updated CODESYS Installer.

The CODESYS Installer as well as the CODESYS Development System can 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 [4].

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

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/Advisory2026-01_INST-1084.pdf

Change History

Version	Description	Date
1.0	Initial version	2026-03-10