CODESYS Visualization - Insufficiently Protected Credentials

CODESYS Security Advisory 2026-07

Published: 2026-05-21

Last Change: 2026-05-21

Identifiers, Type and Severity

CVE-2026-0393

CERT@VDE: VDE-2026-052

CODESYS: VIS-6204

CWE-522: Insufficiently Protected Credentials

CVSS v3.1 Base Score: 5.7 | Medium | CVSS:3.1/AV:N/AC:L/PR:L/UI:R/S:U/C:H/I:N/A:N

1 Summary

A vulnerability in the CODESYS Visualization login dialog has been identified. During logins within the CODESYS Visualization, authentication data may not be sufficiently isolated when multiple users perform login operations concurrently.

As a result, an authenticated visualization user may be able to obtain credentials entered by another visualization user. The issue affects only login operations within an active visualization session and can be triggered via local and remote access to the visualization.

2 Affected Products

The following product is affected in all versions before 4.10.0.0.
• CODESYS Visualization

3 Impact

Exploitation of this vulnerability may allow an authenticated remote visualization user to obtain credentials entered by another visualization user, potentially with higher privileges.

4 Remediation

Update the following product to version 4.10.0.0.
• CODESYS Visualization

For existing affected CODESYS projects that include a visualization, the fix takes effect only after recompiling the application and performing a new download to the HMI or PLC.

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 Mitigation

Two alternative mitigation options have been identified.

One option is to avoid using the Input Action "User Management -> Login" for changing users within an active visualization session. Instead, use the Input Action "User Management -> Logout" to do a complete logout followed by a new Login to the Visualization to re-login with another user.

Alternatively, property handling within the visualization can be disabled via Project Settings -> Visualization -> General -> Advanced -> "Activate property handling in all element properties", if this is not required for the compilation of the application.

6 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.

7 Acknowledgments

This issue was reported by Silvan Schweizer of CTA AG.

Coordination done by CERT@VDE.

CODESYS GmbH thanks all parties involved for their efforts.

8 Further Information

For additional information regarding the CODESYS products, especially the above-mentioned versions, or about the described vulnerability please contact CODESYS support.

9 Disclaimer

10 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/Advisory2026-07_VIS-6204.pdf

Change History

Version	Description	Date
1.0	Initial version	2026-05-21