CODESYS PROFINET Controller - Out-of-bounds Write

CODESYS Security Advisory 2026-06

Published: 2026-07-29

Last Change: 2026-07-29

Identifiers, Type and Severity

CVE-2026-35226
CERT@VDE: VDE-2026-041
CODESYS: PN-927

CWE-787: Out-of-bounds Write

CVSS v3.1 Base Score: 6.5 | Medium | CVSS:3.1/AV:A/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H

1 Summary

CODESYS PROFINET is an add-on for the CODESYS Development System that provides a fully integrated PROFINET protocol stack along with diagnostic capabilities. When a PROFINET Controller is configured, this vulnerable protocol stack is downloaded to and executed by CODESYS Control runtime systems.

The vulnerability in the CODESYS PROFINET Controller is caused by an out-of-bounds write during the processing of received invalid PROFINET communication data. Triggering this condition causes the CODESYS Control runtime system to handle the resulting exception and stop the affected PLC application in a controlled manner. Remote code execution is not considered feasible, as the execution flow remains controlled.

This issue affects only CODESYS projects that include a PROFINET Controller configuration.

2 Affected Products

The following product is affected in all versions from 4.4.0.0 and before 4.8.0.0:
• CODESYS PROFINET

3 Impact

Exploitation of the vulnerability allows an unauthenticated attacker to trigger an exception that is handled by the CODESYS Control runtime system, resulting in a controlled stop of the affected PLC application until it is restarted.

4 Remediation

Update the following product to version 4.8.0.0.
• CODESYS PROFINET

To make the fix effective for existing CODESYS projects, you must additionally update the PROFINET Controller in the device tree to the latest version and perform a download of the CODESYS application to the 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 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 ABB.

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/Advisory2026-06_PN-927.pdf

Change History

Version	Description	Date
1.0	Initial version	2026-07-29