



Feeds

CNA

Report



Advisories

Show filters



VDE-2026-044

May 27, 2026, 1:00 PM

MB connect line: Multiple SQLi vulnerabilities in mbCONNECT24/mymbCONNECT24

Multiple SQLi vulnerabilities have been discovered in MB connect line mbCONNECT24/mymbCONNECT24.

◆ CVE-2026-40850

◆ CVE-2026-40819

◆ CVE-2026-40818

◆ CVE-2026-40817

◆ CVE-2026-40816

◆ CVE-2026-40815

◆ CVE-2026-40814

◆ CVE-2026-40813

◆ CVE-2026-40812

◆ CVE-2026-40811

◆ CVE-2026-40810

◆ CVE-2026-40836

◆ CVE-2026-40834

◆ CVE-2026-40833

● CVE-2026-40849

● CVE-2026-40848

● CVE-2026-40847

● CVE-2026-40846

● CVE-2026-40845

● CVE-2026-40844

● CVE-2026-40843

● CVE-2026-40842

● CVE-2026-40841

● CVE-2026-40840

● CVE-2026-40839

● CVE-2026-40838

● CVE-2026-40837

● CVE-2026-40835

● CVE-2026-40832

● CVE-2026-40831

● CVE-2026-40830

● CVE-2026-40829

● CVE-2026-40828

● CVE-2026-40827

● CVE-2026-40825

● CVE-2026-40824

● CVE-2026-40823

● CVE-2026-40826

● CVE-2026-40822

● CVE-2026-40821

● CVE-2026-40820

VDE-2026-054

May 27, 2026, 1:00 PM

MB connect line: Multiple vulnerabilities in mbNET/mbNET.rokey/mbNET.mini

Two command injection vulnerabilities have been discovered in MB connect line mbNET/mbNET.rokey/mbNET.mini.

◆ CVE-2026-40851

◆ CVE-2026-40852

VDE-2026-059

May 27, 2026, 1:00 PM

Helmholz: Multiple vulnerabilities in REX100/REX200/REX250

Two command injection vulnerabilities have been discovered in Helmholz REX100/REX200/REX250.

◆ CVE-2026-40851

◆ CVE-2026-40852

VDE-2026-058

May 27, 2026, 1:00 PM

Helmholz: Multiple SQLi vulnerabilities in myREX24V2/myREX24V2.virtual

Multiple SQLi vulnerabilities have been discovered in Helmholz myREX24V2/myREX24V2.virtual

- ◆ CVE-2026-40850
- ◆ CVE-2026-40819
- ◆ CVE-2026-40818
- ◆ CVE-2026-40817
- ◆ CVE-2026-40816
- ◆ CVE-2026-40815
- ◆ CVE-2026-40814
- ◆ CVE-2026-40813
- ◆ CVE-2026-40812
- ◆ CVE-2026-40811
- ◆ CVE-2026-40810
- ◆ CVE-2026-40836
- ◆ CVE-2026-40834
- ◆ CVE-2026-40833
- CVE-2026-40849
- CVE-2026-40848
- CVE-2026-40847
- CVE-2026-40846
- CVE-2026-40845
- CVE-2026-40844
- CVE-2026-40843
- CVE-2026-40842
- CVE-2026-40841
- CVE-2026-40840
- CVE-2026-40839
- CVE-2026-40838
- CVE-2026-40837
- CVE-2026-40835
- CVE-2026-40832
- CVE-2026-40831
- CVE-2026-40830
- CVE-2026-40829
- CVE-2026-40828
- CVE-2026-40827
- CVE-2026-40825
- CVE-2026-40824
- CVE-2026-40823
- CVE-2026-40826
- CVE-2026-40822
- CVE-2026-40821
- CVE-2026-40820

Phoenix Contact: PLCnext Firmware Security Issues Related to APPs and Configuration Files

This advisory addresses security issues in PLCnext firmware versions prior to 2026.0.3 that are related to APP handling and the processing of configuration files. The identified vulnerabilities affect APP installation ...

◆ CVE-2025-41669

◆ CVE-2025-41670

VDE-2026-055

May 26, 2026, 12:00 PM

CODESYS Development System - Incorrect Default Permissions

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. ...

◆ CVE-2026-44469

◆ CVE-2026-44468

VDE-2026-056

May 26, 2026, 12:00 PM

CODESYS Control - Incorrect Authorization

The CODESYS Control runtime system provides a user management mechanism with multiple privilege groups including the visualization administrators group, which is intended solely to manage visualization users. Due to insufficient ...

◆ CVE-2026-8046

VDE-2026-057

May 26, 2026, 12:00 PM

CODESYS Control - Out-of-bounds Write

The CmpWebServer component in the CODESYS Control Runtime allows users to create browser-based visualizations for monitoring and controlling industrial processes. Due to improper bounds checking, a specially crafted HTTP request ...

◆ CVE-2026-8047

⏪ < 1 2 3 4 5 ... > ⏩

Contact

Impressum

Data protection notice

Privacy statement

Share this page



© VDE CERT 2026

Member of

