

[Feeds](#)[CNA](#)[Melden](#)[< Zurück zur Übersicht](#)

# MB connect line: Multiple Vulnerabilities in mbCONNECT24/mymbCONNECT24

## VDE-2026-030

Last update	02.04.2026 13:00
Published at	02.04.2026 13:00
Vendor(s)	MB connect line GmbH
External ID	VDE-2026-030
CSAF Document	<a href="#">Download</a> ↗

## Summary

Multiple vulnerabilities have been discovered in MB connect line mbCONNECT24/mymbCONNECT24 that could allow RCE, SQLi or information leakage.

## Impact

CVE-2026-33613 allows RCE resulting in full system compromise impacting confidentiality, integrity, and availability. CVE-2026-33614 and CVE-2026-33616 allow unauthenticated SQLi resulting in arbitrary read access to the complete database, while CVE-2026-33615 results in






arbitrary write access to the user table. Lastly CVE-2026-33617 allows unauthenticated access to some sensitive data.

## Affected Product(s)

Model no.	Product name	Affected versions
	MB connect line mbCONNECT24	Firmware <=2.19.4, Firmware 2.19.4
	mymbCONNECT24	Firmware 2.19.4, Firmware <=2.19.4

## Vulnerabilities

[Expand / Collapse all](#)

CVE-2026-33615	 9.1	∨
CVE-2026-33616	 7.5	∨
CVE-2026-33614	 7.5	∨
CVE-2026-33613	 7.2	∨
CVE-2026-33617	 5.3	∨

## Remediation

Update the mbCONNECT24/mymbCONNECT24 instance to version 2.19.5.

## Acknowledgments

MB connect line GmbH thanks the following parties for their efforts:

- CERT@VDE for coordination (see <https://certvde.com> ↗)
- Moritz Abrell, Christian Zäske from SySS GmbH for reporting (see <https://www.syss.de> ↗)

## Revision History

Version	Date	Summary
1.0.0	02.04.2026 13:00	Initial revision.

**Kontakt**

**Impressum**

**Datenschutzerklärung**

**Datenschutzhinweise**

Diese Seite teilen



© VDE CERT 2026

**Mitglied bei**

