





# Security Incident Management

<b>Incident reported by:</b> LEWA Attendorn GmbH	<b>Date:</b>  22.06.2021
<b>Referenced Documents:</b> VCR-XQEHX-235	
<b>Incidents covered by this document:</b> <ul style="list-style-type: none"> <li>• Vulnerability SIM#2021-04-a: "User enumeration"</li> </ul>	
<b>VDE-ID:</b> VDE-2021-037	
<b>Public disclosure:</b>	<b>Date:</b>
Incident-Report - SIM#2021-04 mbCONNECT24/mymbCONNECT24 - Firmware 2.10.1	 27.10.2021  15.10.2021

 The MB connect line security team can be reached via email at [security-team@mbconnectline.com](mailto:security-team@mbconnectline.com). For incident-reports, please use encrypted communication only. For details and PGP-credentials visit <https://mbconnectline.com/security-advice/>.

More information on current threats and the associated product safety of our devices and software solutions can be found at <https://mbconnectline.com/security-advice/>.

All vulnerability-metrics used in this document are created with the NIST NVD CVSS-Calculator V3 <https://nvd.nist.gov/vuln-metrics/cvss/v3-calculator>

# Vulnerability SIM#2021-04-a: "User enumeration"

## Details

<p><b>CVE:</b> <a href="#">CVE-2021-34580</a></p>
<p><b>Description:</b> An issue was discovered in the mymbCONNECT24 and mbCONNECT24 software in all versions through V2.9.0. An unauthenticated user can enumerate valid backend users by checking what kind of response the server sends for crafted invalid login attempts.</p>
<p><b>Solution:</b> Update to 2.10.1.</p>

## Affected Products

<b>Product:</b>	<b>Version:</b>	<b>Update:</b>
mbCONNECT24, mymbCONNECT24	<= 2.9.0	2.10.1

## CVSS Scores & Vulnerability

<b>CWE-Identifier:</b>	CWE-204
<b>CVSS Base Score:</b>	7.5
<b>CVSS v3 Link:</b>	<a href="#">AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N</a>

**Document:** SIM#2021-04 / Rev.: 6  
**Created by:** fade / 2021-10-27