Security Incident Management

Incident reported by: Hussein Alsharafi	*Date:* 22.02.2023
Referenced Documents: IDOR_POC.webm	
Incidents covered by this document: ▪ Vulnerability SIM#2023-01-a: "Account takeover via password reset"	
VDE-ID: VDE-2023-002	
Public disclosure:	*Date:*
Incident-Report - SIM#2023-01 mbCONNECT24/mymbCONNECT24 - Firmware 2.13.4	15.05.2023 15.03.2023

The MB connect line security team can be reached via email at security-team@mbconnectline.de. For incident-reports, please use encypted 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

MB connect line GmbH
Winnettener Str. 6
D-91550 Dinkelsbühl

+49 (0) 9851 / 58 25 29 0
+49 (0) 9851 / 58 25 29 99
info@mbconnectline.com
www.mbconnectline.com

Vulnerability SIM#2023-01-a:
"Account takeover via password reset"

Details

CVE: CVE-2023-0985
Description: An issue was discovered in the mymbCONNECT24 and mbCONNECT24 software in all versions through V2.13.3. An authenticated user can change the password of any user in the same account by abusing an IDOR issue in the password reset function. This allows to take over the admin user and therefore fully compromise the account.
Solution: Update to latest Version: 2.13.4 **Mitigation**: If you have MFA enabled on the admin user, the password will still be set, but the attacker will be unable to login as the MFA is still in place.

Affected Products

Product:	***Version:***	***Update:***
mbCONNECT24, mymbCONNECT24	<= 2.13.3	2.13.4

CVSS Scores & Vulnerability

CWE-Identifier:	CWE-639
CVSS Base Score:	8.8
CVSS v3 Link:	AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H

Document: SIM#2023-01 / Rev.: 9
Created by:fade / 2023-05-15