Security Incident Management

Incident reported by: OTORIO	***Date:*** 04.05.2023
Incident coordinated by: CERT@VDE	
Incidents covered by this document: ▪ Vulnerability SIM#2023-03-a: "Inproper access validation"	
VDE-ID: VDE-2023-041	
Public disclosure:	***Date:***
Incident-Report - SIM#2023-03 mbCONNECT24/mymbCONNECT24 2.14.3	16.10.2023 14.09.2023

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

Document: SIM#2023-03 / Rev.: 4
Created by:fade / 2023-10-16

Red Lion Europe GmbH
Winnettener Str. 6
91550 Dinkelsbühl
GERMANY
+49 (0) 98 51 / 58 25 29 0
+49 (0) 98 51 / 58 25 29 99
info@mbconnectline.com
www.mbconnectline.com

Vulnerability SIM#2023-03-a: "Inproper access validation"

Details

CVE: CVE-2023-4834
Description: An issue was discovered in the mymbCONNECT24 and mbCONNECT24 software in all versions through V2.14.2. An inproperly implemented access validation allows an authenticated, low privileged attacker to gain read access to limited, non-critical device information in his account he should not have access to.
Solution: Update to latest Version: 2.14.3

Affected Products

Product:	***Version:***	***Update:***
mbCONNECT24, mymbCONNECT24	<= 2.14.2	2.12.1

CVSS Scores & Vulnerability

CWE-Identifier:	CWE-269
CVSS Base Score:	4.3
CVSS v3 Link:	AV:N/AC:L/PR:L/UI:N/S:U/C:L/I:N/A:N

Document: SIM#2023-03 / Rev.: 4
Created by:fade / 2023-10-16

Red Lion Europe GmbH
Winnettener Str. 6
91550 Dinkelsbühl
GERMANY
+49 (0) 98 51 / 58 25 29 0
+49 (0) 98 51 / 58 25 29 99
info@mbconnectline.com
www.mbconnectline.com