Security Incident Management

Incident reported by: Helmholz GmbH & Co. KG	*Date:* 📅 09.02.2023
Referenced Documents: NFP-SBZWW-285	
Incidents covered by this document: ▪ Vulnerability SIM#2023-02-a: "Information Leak"	
VDE-ID: VDE-2023-002	

Public disclosure:	*Date:*
Incident-Report - SIM#2023-02 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

Vulnerability SIM#2023-02-a: "Information Leak"

Details

CVE: CVE-2023-1779
Description: An issue was discovered in the mymbCONNECT24 and mbCONNECT24 software in all versions through V2.13.3. An incorrectly implemented object cache in the task scheduler allow an authorized remote attacker with low privileges to view a limited amount of another accounts contact information.
Solution: Update to latest Version: 2.13.4

Affected Products

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

CVSS Scores & Vulnerability

CWE-Identifier:	CWE-200
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#2023-02 / Rev.: 4
Created by:fade / 2023-05-15