Security Incident Management

Incident reported by: Red Lion Inc.	***Date:*** 20.11.2023
Incident coordinated by: CERT@VDE	
Incidents covered by this document: ▪ Vulnerability SIM#2023-06-a: "Unencrypted configuration file" ▪ Vulnerability SIM#2023-06-b: "Missing authorization in data24"	
VDE-ID: VDE-2024-010	

Public disclosure:	***Date:***
Incident-Report - SIM#2023-06 mbCONNECT24/mymbCONNECT24 2.16.2	18.03.2025 24.07.2024

ⓘ 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#2023-06-a:
"Unencrypted configuration file"

Details

CVE: CVE-2024-23942
Description: A local user may find a configuration file on the client workstation with unencrypted sensitive data. This allows an attacker to impersonate the device or prevent the device from accessing the cloud portal which leads to a DoS.
Solution: **Workaround**: Prefill the devices serial number and delete the configuration file immediately after applying. **Remediation**: Update to latest Version: 2.16.2

Affected Products

Product:	***Version:***	***Update:***
mbCONNECT24, mymbCONNECT24	<= 2.16.1	2.16.2

CVSS Scores & Vulnerability

CWE-Identifier:	CWE-311
CVSS Base Score:	7.1
CVSS v3 Link:	AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:H

Vulnerability SIM#2023-06-b: "Missing authorization in data24"

Details

CVE: CVE-2024-23943
Description: An unauthenticated remote attacker can gain access to the cloud API due to a lack of authentication for a critical function in the affected devices. Availability is not affected.
Solution: Update to latest Version: 2.16.2 **ATTENTION:** This fix does not apply to mbNET/mbNET.rokey devices with firmware 8.0.0 - 8.1.3. If you are using a device with this firmware, please update it to >= 8.2.0.

Affected Products

Product:	***Version:***	***Update:***
mbCONNECT24, mymbCONNECT24	<= 2.16.1	2.16.2

CVSS Scores & Vulnerability

CWE-Identifier:	CWE-306
CVSS Base Score:	9.1
CVSS v3 Link:	AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:N

Document: SIM#2023-06 / Rev.: 8
Created by:fade / 2025-03-18