Security Incident Management

Incident reported by:	*Date:*
OTORIO	16.07.2020

Referenced Documents:

OTORIO-MBCONNECT DISCLOSURE.zip

Incidents covered by this document:

- Vulnerability SIM#2021-02-a: "Client-side password policy validation"
- Vulnerability SIM#2021-02-b: "User enumeration"

VDE-ID:

VDE-2021-030

Public disclosure:	*Date:*
Incident-Report - SIM#2021-02	22.07.2021
mbCONNECT24/mymbCONNECT24 - Firmware 2.9.0	27.05.2021

The MB connect line security team can be reached via email at security-team@mbconnectline.com. For incident-reports, please use encypted communication only. For details and PGP-credentials visit https://www.mbconnectline.de/de/support/sicherheitshinweise.html.

More information on current threats and the associated product safety of our devices and software solutions can be found at https://www.mbconnectline.de/de/support/sicherheitshinweise.html.

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#2021-02 / Rev.: 6
Created by:fade / 2021-07-22

Vulnerability SIM#2021-02-a:
"Client-side password policy validation"

Details

CVE: CVE-2021-34574
Description: An issue was discovered in the mymbCONNECT24 and mbCONNECT24 software in all versions through V2.8.0. An authenticated attacker can change the password of his account into a new password that violates the password policy by intercepting and modifying the request that is send to the server.
Solution: Update to 2.9.0.

Affected Products

Product:	*Version:*	*Update:*
mbCONNECT24, mymbCONNECT24	<= 2.8.0	2.9.0

CVSS Scores & Vulnerability

CWE-Identifier:	CWE-669
CVSS Base Score:	4.3
CVSS v3 Link:	AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:L/A:N

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#2021-02-b:
"User enumeration"

Details

CVE: CVE-2021-34575
Description: An issue was discovered in the mymbCONNECT24 and mbCONNECT24 software in all versions through V2.8.0. An unauthenticated user can enumerate valid users by checking what kind of response the server sends.
Solution: Update to 2.9.0.

Affected Products

Product:	*Version:*	*Update:*
mbCONNECT24, mymbCONNECT24	<= 2.8.0	2.9.0

CVSS Scores & Vulnerability

CWE-Identifier:	CWE-204
CVSS Base Score:	7.5
CVSS v3 Link:	AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N

Document: SIM#2021-02 / Rev.: 6
Created by:fade / 2021-07-22