Security Incident Management

Incident reported by:	*Date:*
OTORIO	13.04.2022

Referenced Documents:
MB Connect retest report - final.pdf

Incidents covered by this document:
- Vulnerability SIM#2022-02-a: "Inproper access validation"
- Vulnerability SIM#2022-02-b: "Information Disclosure"
- Vulnerability SIM#2022-02-c: "Server-side request forgery (SSRF)"
- Vulnerability SIM#2022-02-d: "Client-side password policy validation"
- Vulnerability SIM#2022-02-e: "Local file inclusion (LFI)"
- Vulnerability SIM#2022-02-f: "Inproper access validation"
- Vulnerability SIM#2022-02-g: "Information Disclosure"

VDE-ID:
VDE-2021-003
VDE-2021-030

Public disclosure:	*Date:*
Incident-Report - SIM#2022-02 mbCONNECT24/mymbCONNECT24 - Firmware 2.12.1	07.09.2022 16.08.2022

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://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#2022-02-a: "Inproper access validation"

Details

CVE: CVE-2020-35557
Description: An issue was discovered in the mymbCONNECT24 and mbCONNECT24 software in all versions through V2.11.2. An incomplete fix for CVE-2020-35557 allows an authenticated attacker to gain read access to device data that should not be accessable by him in some non default ACL setups.
Solution: Update to latest Version: 2.12.1

Affected Products

Product:	***Version:***	***Update:***
mbCONNECT24, mymbCONNECT24	<= 2.11.2	2.12.1

CVSS Scores & Vulnerability

CWE-Identifier:	CWE-269
CVSS Base Score:	6.5
CVSS v3 Link:	AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:N/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#2022-02-b: "Information Disclosure"

Details

CVE: CVE-2020-35570
Description: An issue was discovered in the mymbCONNECT24 and mbCONNECT24 software in all versions through V2.11.2. An incomplete fix to CVE-2020-35570 allows an attacker to access files (that should have been restricted) via forceful browsing.
Solution: Update to latest Version: 2.12.1

Affected Products

Product:	***Version:***	***Update:***
mbCONNECT24, mymbCONNECT24	<= 2.11.2	2.12.1

CVSS Scores & Vulnerability

CWE-Identifier:	CWE-552
CVSS Base Score:	5.3
CVSS v3 Link:	AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/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#2022-02-c:
"Server-side request forgery (SSRF)"

Details

CVE: CVE-2020-35558
Description: An issue was discovered in the mymbCONNECT24 and mbCONNECT24 software in all versions through V2.11.2. An incomplete fix to CVE-2020-35558 allows an attacker to scan some networks for open ports.
Solution: Update to latest Version: 2.12.1

Affected Products

Product:	*Version:*	*Update:*
mbCONNECT24, mymbCONNECT24	<= 2.11.2	2.12.1

CVSS Scores & Vulnerability

CWE-Identifier:	CWE-918
CVSS Base Score:	5.8
CVSS v3 Link:	AV:N/AC:L/PR:N/UI:N/S:C/C:L/I:N/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#2022-02-d:
"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 V2.11.2. An authenticated attacker can change the password of a device into a new password that violates the password policy by intercepting and modifying the request that is send to the server. This is an update for CVE-2021-34574 which addressed the same issue at another place.
Solution: Update to latest Version: 2.12.1

Affected Products

Product:	***Version:***	***Update:***
mbCONNECT24, mymbCONNECT24	<= 2.11.2	2.12.1

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#2022-02-e: "Local file inclusion (LFI)"

Details

CVE: CVE-2020-35566
Description: An issue was discovered in the mymbCONNECT24 and mbCONNECT24 software in all versions through V2.11.2. An incomplete fix to CVE-2020-35566 allows an attacker to read arbitrary JSON files via Local File Inclusion.
Solution: Update to latest Version: 2.12.1

Affected Products

Product:	***Version:***	***Update:***
mbCONNECT24, mymbCONNECT24	<= 2.11.2	2.12.1

CVSS Scores & Vulnerability

CWE-Identifier:	CWE-98
CVSS Base Score:	5.3
CVSS v3 Link:	AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/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#2022-02-f:
"Inproper access validation"

Details

CVE: CVE-2020-12527
Description: An issue was discovered in the mymbCONNECT24 and mbCONNECT24 software in all versions through V2.11.2. An incomplete fix to CVE-2020-12527 allows an authenticated attacker to interact with a device that should not be accessable by him in some non default ACL setups.
Solution: Update to latest Version: 2.12.1

Affected Products

Product:	*Version:*	*Update:*
mbCONNECT24, mymbCONNECT24	<= 2.11.2	2.12.1

CVSS Scores & Vulnerability

CWE-Identifier:	CWE-98
CVSS Base Score:	5.3
CVSS v3 Link:	AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N

Document: SIM#2022-02 / Rev.: 6
Created by:fade / 2022-09-07

Vulnerability SIM#2022-02-g: "Information Disclosure"

Details

CVE: CVE-2020-35568
Description: An issue was discovered in the mymbCONNECT24 and mbCONNECT24 software in all versions through V2.11.2. An incomplete fix to CVE-2020-35568 allows an authenticated attacker to gain read access to userdata that should not be accessable by him.
Solution: Update to latest Version: 2.12.1

Affected Products

Product:	***Version:***	***Update:***
mbCONNECT24, mymbCONNECT24	<= 2.11.2	2.12.1

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

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