SIM#2020-04-2

Security Incident Management

Incident reported by:	*Date:*
OTORIO	16.07.2020

Referenced Documents:

OTORIO-MBCONNECT DISCLOSURE.zip

Incidents covered by this document:

- Vulnerability SIM#2020-04-2-a: "Inproper access validation"
- Vulnerability SIM#2020-04-2-b: "Inproper access validation"
- Vulnerability SIM#2020-04-2-c: "Inproper access validation"
- Vulnerability SIM#2020-04-2-d: "Sensitive information disclosure"
- Vulnerability SIM#2020-04-2-e: "Server-side request forgery (SSRF)"
- Vulnerability SIM#2020-04-2-f: "Server-side request forgery (SSRF)"
- Vulnerability SIM#2020-04-2-g: "Open redirect"
- Vulnerability SIM#2020-04-2-h: "Cross-Site-Scripting (XSS)"
- Vulnerability SIM#2020-04-2-i: "Cross-Site-Scripting (XSS)"
- Vulnerability SIM#2020-04-2-j: "Cross-Site-Scripting (XSS)"
- Vulnerability SIM#2020-04-2-k: "Cross-Site-Scripting (XSS)"
- Vulnerability SIM#2020-04-2-l: "Local file inclusion (LFI)"
- Vulnerability SIM#2020-04-2-m: "Denial of service"
- Vulnerability SIM#2020-04-2-n: "Unfiltered database queries"
- Vulnerability SIM#2020-04-2-o: "Shared password"
- Vulnerability SIM#2020-04-2-p: "Weak default configuration"
- Vulnerability SIM#2020-04-2-q: "Server-side request forgery (SSRF)"
- Vulnerability SIM#2020-20-2-r: "Local Privilege Escalation"

VDE-ID:

VDE-2021-003

Public disclosure:	*Date:*
Incident-Report - SIM#2020-04-1	15.02.2021
mbCONNECT24/mymbCONNECT24	07.12.2020

Document: SIM#2020-04-2 / Rev.: 28
Created by: fade / 2021-02-15

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#2020-04-2-a:
"Inproper access validation"

Details

CVE: CVE-2020-35557
Description: An issue was discovered in the mymbCONNECT24 and mbCONNECT24 software in all versions through V2.6.2. Inproper use of access validation allows a logged in user to see devices in the account he should not have access to.
Solution: Update to 2.7.1

Affected Products

Product:	*Version:*	*Update:*
mbCONNECT24, mymbCONNECT24	<=2.6.2	2.7.1

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#2020-04-2-b:
"Inproper access validation"

Details

CVE: CVE-2020-12527
Description: An issue was discovered in the mymbCONNECT24 and mbCONNECT24 software in all versions through V2.6.2. Inproper use of access validation allows a logged in user to interact with devices in the account he should not have access to.
Solution: Update to 2.7.1

Affected Products

Product:	*Version:*	*Update:*
mbCONNECT24, mymbCONNECT24	<=2.6.2	2.7.1

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:N/I:N/A:H

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#2020-04-2-c:
"Inproper access validation"

Details

CVE: CVE-2020-12528
Description: An issue was discovered in the mymbCONNECT24 and mbCONNECT24 software in all versions through V2.6.2. Inproper use of access validation allows a logged in user to kill web2go sessions in the account he should not have access to.
Solution: Update to 2.7.1

Affected Products

Product:	*Version:*	*Update:*
mbCONNECT24, mymbCONNECT24	<=2.6.2	2.7.1

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:N/I:N/A:H

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#2020-04-2-d:
"Sensitive information disclosure"

Details

CVE: CVE-2020-35570
Description: An issue was discovered in the mymbCONNECT24 and mbCONNECT24 software in all versions through V2.6.2. An unauthenticated attacker is able to access files (that should have been restricted) via forceful browsing.
Solution: Update to 2.7.1

Affected Products

Product:	*Version:*	*Update:*
mbCONNECT24, mymbCONNECT24	<=2.6.2	2.7.1

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#2020-04-2-e:
"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 V2.6.2 There is a SSRF in the MySQL access check, allowing an attacker to scan for open ports and gain some information about possible credentials.
Solution: Update to 2.7.1

Affected Products

Product:	*Version:*	*Update:*
mbCONNECT24, mymbCONNECT24	<=2.6.2	2.7.1

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#2020-04-2-f:
"Server-side request forgery (SSRF)"

Details

CVE: CVE-2020-12529
Description: An issue was discovered in the mymbCONNECT24 and mbCONNECT24 software in all versions through V2.6.2 There is a SSRF in the LDAP access check, allowing an attacker to scan for open ports.
Solution: Update to 2.7.1

Affected Products

Product:	*Version:*	*Update:*
mbCONNECT24, mymbCONNECT24	<=2.6.2	2.7.1

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#2020-04-2-g:
"Open redirect"

Details

CVE: CVE-2020-35560
Description: An issue was discovered in the mymbCONNECT24 and mbCONNECT24 software in all versions through V2.6.2. There is an unauthenticated open redirect in the redirect.php.
Solution: Update to 2.7.1

Affected Products

Product:	*Version:*	*Update:*
mbCONNECT24, mymbCONNECT24	<=2.6.2	2.7.1

CVSS Scores & Vulnerability

CWE-Identifier:	CWE-601
CVSS Base Score:	4.3
CVSS v3 Link:	AV:N/AC:L/PR:N/UI:R/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#2020-04-2-h:
"Cross-Site-Scripting (XSS)"

Details

CVE: CVE-2020-12530
Description: An issue was discovered in the mymbCONNECT24 and mbCONNECT24 software in all versions through V2.6.2. There is an XSS issue in the redirect.php allowing an attacker to inject code via a get parameter.
Solution: Update to 2.7.1

Affected Products

Product:	*Version:*	*Update:*
mbCONNECT24, mymbCONNECT24	<=2.6.2	2.7.1

CVSS Scores & Vulnerability

CWE-Identifier:	CWE-79
CVSS Base Score:	4.3
CVSS v3 Link:	AV:N/AC:L/PR:N/UI:R/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#2020-04-2-i:
"Cross-Site-Scripting (XSS)"

Details

CVE: CVE-2020-35563
Description: An issue was discovered in the mymbCONNECT24 and mbCONNECT24 software in all versions through V2.6.2. There is an incomplete XSS filter allowing an attacker to inject specically crafted malicious code into the page.
Solution: Update to 2.7.1

Affected Products

Product:	*Version:*	*Update:*
mbCONNECT24, mymbCONNECT24	<=2.6.2	2.7.1

CVSS Scores & Vulnerability

CWE-Identifier:	CWE-79
CVSS Base Score:	3.5
CVSS v3 Link:	AV:N/AC:L/PR:L/UI:R/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#2020-04-2-j:
"Cross-Site-Scripting (XSS)"

Details

CVE: CVE-2020-35564
Description: An issue was discovered in the mymbCONNECT24 and mbCONNECT24 software in all versions through V2.6.2. There is an outdated and unused component allowing for malicious user input of active code.
Solution: Update to 2.7.1

Affected Products

Product:	*Version:*	*Update:*
mbCONNECT24, mymbCONNECT24	<=2.6.2	2.7.1

CVSS Scores & Vulnerability

CWE-Identifier:	CWE-79
CVSS Base Score:	4.3
CVSS v3 Link:	AV:N/AC:L/PR:N/UI:R/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#2020-04-2-k: "Cross-Site-Scripting (XSS)"

Details

CVE: CVE-2020-35569
Description: An issue was discovered in the mymbCONNECT24 and mbCONNECT24 software in all versions through V2.6.2. There is a self XSS issue with a crafted cookie in the login page.
Solution: Update to 2.7.1

Affected Products

Product:	*Version:*	*Update:*
mbCONNECT24, mymbCONNECT24	<=2.6.2	2.7.1

CVSS Scores & Vulnerability

CWE-Identifier:	CWE-79
CVSS Base Score:	3.3
CVSS v3 Link:	AV:L/AC:L/PR:N/UI:R/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#2020-04-2-I:
"Local file inclusion (LFI)"

Details

CVE: CVE-2020-35566
Description: An issue was discovered in the mymbCONNECT24 and mbCONNECT24 software in all versions through V2.6.2. An attacker can read arbitrary JSON files via Local File Inclusion.
Solution: Update to 2.7.1

Affected Products

Product:	*Version:*	*Update:*
mbCONNECT24, mymbCONNECT24	<=2.6.2	2.7.1

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#2020-04-2-m:
"Denial of service"

Details

CVE: CVE-2020-35559
Description: An issue was discovered in the mymbCONNECT24 and mbCONNECT24 software in all versions through V2.6.2. There is an unused function that allows an authenticated attacker to use up all available IPs of an account and thus not allowing to create new devices and users.
Solution: Update to 2.7.1

Affected Products

Product:	*Version:*	*Update:*
mbCONNECT24, mymbCONNECT24	<=2.6.2	2.7.1

CVSS Scores & Vulnerability

CWE-Identifier:	CWE-400
CVSS Base Score:	4.3
CVSS v3 Link:	AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:L

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#2020-04-2-n:
"Unfiltered database queries"

Details

CVE: CVE-2020-35568
Description: An issue was discovered in the mymbCONNECT24 and mbCONNECT24 software in all versions through V2.6.2. An incomplete filter applied to a database response allows an authenticated attacker to gain non public information about other users and devices in the account. **No security relevant information was accessable!**
Solution: Update to 2.7.1

Affected Products

Product:	*Version:*	*Update:*
mbCONNECT24, mymbCONNECT24	<=2.6.2	2.7.1

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

Vulnerability SIM#2020-04-2-o:
"Shared password"

Details

CVE: CVE-2020-35567
Description: An issue was discovered in the mymbCONNECT24 and mbCONNECT24 software in all versions through V2.6.2. The software uses a secure password for database access, but this password is shared between instances.
Solution: None (A proper fix for the underlying issue will come with a future architectural core-system-update) ***Workaround:*** No way of exploit known.

Affected Products

Product:	*Version:*	*Update:*
mbCONNECT24, mymbCONNECT24	all	none

CVSS Scores & Vulnerability

CWE-Identifier:	CWE-798
CVSS Base Score:	7.8
CVSS v3 Link:	AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H

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#2020-04-2-p:
"Weak default configuration"

Details

CVE: CVE-2020-35565
Description: An issue was discovered in the mymbCONNECT24 software in all versions through V2.6.2. The login pages bruteforce detection is disabled by default.
Solution: None (A proper fix for the underlying issue will come with a future update) ***Workaround:*** Activate bruteforce detection via Security → Fail2Ban → WebLogin

Affected Products

Product:	*Version:*	*Update:*
mymbCONNECT24	all	none

CVSS Scores & Vulnerability

CWE-Identifier:	CWE-1188
CVSS Base Score:	5.9
CVSS v3 Link:	AV:N/AC:H/PR:N/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#2020-04-2-q:
"Server-side request forgery (SSRF)"

Details

CVE: CVE-2020-35561
Description: An issue was discovered in the mymbCONNECT24 and mbCONNECT24 software in all versions through V2.6.2. There is a SSRF in the HA module allowing an unauthenticated attacker to scan for open ports.
Solution: None (A proper fix for the underlying issue will come with a future architectural core-system-update) ***Workaround:*** Avoid vulnerable open ports on the LAN side of the server by using a firewall solution

Affected Products

Product:	*Version:*	*Update:*
mbCONNECT24, mymbCONNECT24	all	none

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#2020-20-2-r:
"Local Privilege Escalation"

Details

CVE: CVE-2020-10384
Description: An issue was discovered in the mymbCONNECT24 and mbCONNECT24 software in all versions through V2.6.1. There is a local privilege escalation from the www-data account to the root account.
Solution: none (A proper fix for the underlying issue will come with a future architectural core-system-update) ***Workaround:*** Update to version 2.6.2 to close any known way to get to www-data.

Affected Products

Product:	*Version:*	*Update:*
mbCONNECT24, mymbCONNECT24	<=2.6.1	2.6.2

CVSS Scores & Vulnerability

CWE-Identifier:	CWE-269
CVSS Base Score:	7.8
CVSS v3 Link:	AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H

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