SIM#2020-01

Security Incident Management

Incident reported by:	*Date:*
Coesia S.p.A. / CY4 Gate	14.02.2020

Referenced Documents:

CY4/19-DEL069 - Security Penetration Test on Industrial Control System

Incidents covered by this document:

- Vulnerability SIM#2020-01-a: "authenticated RCE on mbConnect service"
- Vulnerability SIM#2020-01-b: "unauthenticated SQL injection on mbConnect service"
- Vulnerability SIM#2020-01-c: "unauthenticated RCE on mbConnect service"
- Vulnerability SIM#2020-01-d: "local Privilege Escalation on mbConnect server"

Public disclosure:	*Date:*
Incident-Report - SIM#2020-01	14.04.2020
mbCONNECT24, mymbCONNECT24 Update V2.5.1	26.03.2020

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

Document: SIM#2020-01 / Rev.: 49
Created by: fade / 2020-09-30

Vulnerability SIM#2020-01-a:
"authenticated RCE on mbConnect service"

Details

CVE: CVE-2020-10382
Description: An issue was discovered in the mymbCONNECT24 and mbCONNECT24 software in all versions through V2.5.0. There is an authenticated remote code execution in the backup-scheduler.
Solution: Update to latest Version: 2.5.1

Affected Products

Product:	*Version:*	*Update:*
mbCONNECT24, mymbCONNECT24	<=2.5.0	2.5.1

CVSS Scores & Vulnerability

CVSS Base Score:	7.2
Impact Subscore:	5.9
Exploitability Subscore:	1.2
CVSS v3.1 Vector:	AV:N/AC:L/PR:H/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#2020-01-b:
"unauthenticated SQL injection on mbConnect service"

Details

CVE: CVE-2020-10381
Description: An issue was discovered in the mymbCONNECT24 and mbCONNECT24 software in all versions through V2.5.0. There is an unauthenticated SQL injection in DATA24, allowing attackers to discover database and table names.
Solution: Update to latest Version: 2.5.1

Affected Products

Product:	*Version:*	*Update:*
mbCONNECT24, mymbCONNECT24	<=2.5.0	2.5.1

CVSS Scores & Vulnerability

CVSS Base Score:	5.3
Impact Subscore:	1.4
Exploitability Subscore:	3.9
CVSS v3.1 Vector:	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#2020-01-c:
"unauthenticated RCE on mbConnect service"

Details

CVE: CVE-2020-10383
Description: An issue was discovered in the mymbCONNECT24 and mbCONNECT24 software in all versions through V2.5.0. There is an unauthenticated remote code execution in the com_mb24sysapi module.
Solution: Update to latest Version: 2.5.1

Affected Products

Product:	*Version:*	*Update:*
mbCONNECT24, mymbCONNECT24	<=2.5.0	2.5.1

CVSS Scores & Vulnerability

CVSS Base Score:	9.8
Impact Subscore:	5.9
Exploitability Subscore:	3.9
CVSS v3.1 Vector:	AV:N/AC:L/PR:N/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#2020-01-d:
"local Privilege Escalation on mbConnect server"

Details

CVE: CVE-2020-10384
Description: An issue was discovered in the mymbCONNECT24 and mbCONNECT24 software in all versions through V2.5.0. There is a local privilege escalation from the www-data account to the root account.
Solution: none ***Workaround:*** Update to version 2.5.1 to close any known way to get to www-data. A proper fix for the underlying issue will come with a future architectural core-system-update.

Affected Products

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

CVSS Scores & Vulnerability

CVSS Base Score:	7.8
Impact Subscore:	5.9
Exploitability Subscore:	1.8
CVSS v3.1 Vector:	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