SIM#2020-04-1

Security Incident Management

Incident reported by:	*Date:*
OTORIO	16.07.2020
Referenced documents:	
OTORIO-MBCONNECT DISCLOSURE.zip	
Incidents covered by this document:	
• Vulnerability SIM#2020-04-1-a: "blind SQL injection on mbConnect service" • Vulnerability SIM#2020-04-1-b: "blind SQL injection on mbConnect service" • Vulnerability SIM#2020-04-1-c: "SSRF/CSRF on mbConnect service" • Vulnerability SIM#2020-04-1-d: "unauthenticated RCE on mbConnect service"	
VDE-ID:	
VDE-2020-035	
Public disclosure:	***Date:***
Incident-Report - SIM#2020-04-1 mbCONNECT24/mymbCONNECT24	18.09.2020 20.08.2020

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

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#2020-04-1-a:
"blind SQL injection on mbConnect service"

Details

CVE: CVE-2020-24569
Description: An issue was discovered in the mymbCONNECT24 and mbCONNECT24 software in all versions through V2.6.1. There is a blind SQL injection in the knximport component via an advanced attack vector, allowing logged in attackers to discover arbitrary information. This issue can be completely mitigated regarding remote attackers by using a restrictive external firewall.
Solution: Update to latest Version: 2.6.2

Affected Products

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

CVSS Scores & Vulnerability

CVSS Base Score:	7.1
Impact Subscore:	4.2
Exploitability Subscore:	2.8
CVSS v3 Link:	AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:L

Document: SIM#2020-04-1 / Rev.: 30
Created by: fade / 2020-09-30

Vulnerability SIM#2020-04-1-b:
"blind SQL injection on mbConnect service"

Details

CVE: CVE-2020-24568
Description: An issue was discovered in the mymbCONNECT24 and mbCONNECT24 software in all versions through V2.6.1. There is a blind SQL injection in the lancompenent component, allowing logged in attackers to discover arbitrary information.
Solution: Update to latest Version: 2.6.2

Affected Products

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

CVSS Scores & Vulnerability

CVSS Base Score:	7.1
Impact Subscore:	4.2
Exploitability Subscore:	2.8
CVSS v3 Link:	AV:N/AC:L/PR:L/UI:N/S:U/C:H/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#2020-04-1-c:
"SSRF/CSRF on mbConnect service"

Details

CVE: CVE-2020-24570
Description: An issue was discovered in the mymbCONNECT24 and mbCONNECT24 software in all versions through V2.6.1. There is a SSRF and CSRF issue, in the com_mb24proxy module, allowing attackers to steal session information from logged in users with a specifically crafted link.
Solution: Update to latest Version: 2.6.2

Affected Products

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

CVSS Scores & Vulnerability

CVSS Base Score:	8.8
Impact Subscore:	5.9
Exploitability Subscore:	2.8
CVSS v3 Link:	AV:N/AC:L/PR:N/UI:R/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#2020-04-1-d:
"unauthenticated RCE on mbConnect service"

Details

CVE:
No CVE assigned
Description:
An issue was discovered in the mymbCONNECT24 and mbCONNECT24 software in all versions through V2.6.1. An attacker could use an outdated and unused third party software bundled with the software to gain RCE via an exploit chain.
Solution:
Update to latest Version: 2.6.2

Affected Products

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

CVSS Scores & Vulnerability

CVSS Base Score:	9.8
Impact Subscore:	5.9
Exploitability Subscore:	3.9
CVSS v3 Link:	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