Security Incident Management

Incident reported by: Moritz Abrell of SySS GmbH	*Date:* 25.07.2024
Incident coordinated by: CERT@VDE	
Incidents covered by this document: ▪ Vulnerability SIM#2024-04-a: "RCE via bundled runtime" ▪ Vulnerability SIM#2024-04-b: "Weak credentials" ▪ Vulnerability SIM#2024-04-c: "Weak encryption of configuration" ▪ Vulnerability SIM#2024-04-d: "RCE via confnet service" ▪ Vulnerability SIM#2024-04-e: "RCE via webservice" ▪ Vulnerability SIM#2024-04-f: "tmp directory exposed via webservice"	
VDE-ID: VDE-2024-056 VDE-2024-068	

Public disclosure:	*Date:*
Incident-Report - SIM#2024-04	15.10.2024
mbNET.mini Firmware 2.3.1	09.09.2024
mbNET/mbNET.rokey Firmware 8.3.0	06.09.2024
mbCONNECT24/mymbCONNECT24 Firmware 2.16.3	19.09.2024

The MB connect line security team can be reached via email at security-team@mbconnectline.de. 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

Red Lion Europe GmbH
Winnettener Str. 6
91550 Dinkelsbühl
GERMANY

+49 (0) 98 51 / 58 25 29 0
+49 (0) 98 51 / 58 25 29 99
info@mbconnectline.com
www.mbconnectline.com

Vulnerability SIM#2024-04-a: "RCE via bundled runtime"

Details

CVE: CVE-2024-45271
Description: The configuration file for the mbNET.mini comes bundled with a runtime written in LUA. That runtime is executed with root privileges after applying the configuration. No validation on the content of the runtime is done.
Solution: Update to latest version: 2.3.1

Affected Products

Product:	*Version:*	*Update:*
mbNET.mini	<= 2.2.13	2.3.1

CVSS Scores & Vulnerability

CWE-Identifier:	CWE-20
CVSS Base Score:	8.4
CVSS v3 Link:	AV:L/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

Document: SIM#2024-04 / Rev.: 4
Created by:fade / 2024-10-21

Red Lion Europe GmbH
Winnettener Str. 6
91550 Dinkelsbühl
GERMANY

+49 (0) 98 51 / 58 25 29 0
+49 (0) 98 51 / 58 25 29 99
info@mbconnectline.com
www.mbconnectline.com

Vulnerability SIM#2024-04-b: "Weak credentials"

Details

CVE: CVE-2024-45272
Description: Multiple remote access devices use weak default credentials that are generated by the cloud service. Even though this is a password only used for the first connection it should be secure by default.
Solution: Update to latest version: 2.16.3

Affected Products

Product:	*Version:*	*Update:*
mbCONNECT24, mymbCONNECT24	<= 2.16.2	2.16.3

CVSS Scores & Vulnerability

CWE-Identifier:	CWE-261
CVSS Base Score:	7.5
CVSS v3 Link:	AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H

Red Lion Europe GmbH
Winnettener Str. 6
91550 Dinkelsbühl
GERMANY

+49 (0) 98 51 / 58 25 29 0
+49 (0) 98 51 / 58 25 29 99
info@mbconnectline.com
www.mbconnectline.com

Vulnerability SIM#2024-04-c:
"Weak encryption of configuration"

Details

CVE: CVE-2024-45273
Description: Multiple remote access devices implement a weak encryption scheme with an easily guessable key.
Solution: **mbNET.mini**: Update to 2.3.1 **mbNET/mbNET.rokey**: Update to 8.3.0 **mbCONNECT24/mymbCONNECT24**: Update to 2.16.3 **mbNET HW1/mbSPIDER**: Contact Sales for replacement options

Affected Products

Product:	*Version:*	*Update:*
mbNET.mini mbNET/mbNET.rokey mbNET HW1 mbSPIDER mbCONNECT24, mymbCONNECT24	<= 2.2.13 <= 8.2.0 <= 5.1.11 <= 2.6.5 <= 2.16.2	2.3.1 8.2.1 EOL EOL 2.16.3

CVSS Scores & Vulnerability

CWE-Identifier:	CWE-1391
CVSS Base Score:	8.4
CVSS v3 Link:	AV:L/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

Document: SIM#2024-04 / Rev.: 4
Created by:fade / 2024-10-21

Red Lion Europe GmbH
Winnettener Str. 6
91550 Dinkelsbühl
GERMANY

+49 (0) 98 51 / 58 25 29 0
+49 (0) 98 51 / 58 25 29 99
info@mbconnectline.com
www.mbconnectline.com

Vulnerability SIM#2024-04-d: "RCE via confnet service"

Details

CVE: CVE-2024-45274
Description: The mbNET.mini device exposes an UDP port for a service allowing configuration via the LAN network. This service has unnecessary capabilities that can be exploited to gain RCE as root.
Solution: Update to latest version: 2.3.1

Affected Products

Product:	*Version:*	*Update:*
mbNET.mini	<= 2.2.13	2.3.1

CVSS Scores & Vulnerability

CWE-Identifier:	CWE-306
CVSS Base Score:	9.8
CVSS v3 Link:	AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

Red Lion Europe GmbH
Winnettener Str. 6
91550 Dinkelsbühl
GERMANY

+49 (0) 98 51 / 58 25 29 0
+49 (0) 98 51 / 58 25 29 99
info@mbconnectline.com
www.mbconnectline.com

Vulnerability SIM#2024-04-e: "RCE via webservice"

Details

CVE: CVE-2024-45275
Description: The mbNET.mini device exposes configuration utilities via its webservice that allow RCE. These utilities are only protected by hardcoded passwords.
Solution: Update to latest version: 2.3.1

Affected Products

Product:	*Version:*	*Update:*
mbNET.mini	<= 2.2.13	2.3.1

CVSS Scores & Vulnerability

CWE-Identifier:	CWE-798
CVSS Base Score:	9.8
CVSS v3 Link:	AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

Document: SIM#2024-04 / Rev.: 4
Created by:fade / 2024-10-21

Red Lion Europe GmbH
Winnettener Str. 6
91550 Dinkelsbühl
GERMANY

+49 (0) 98 51 / 58 25 29 0
+49 (0) 98 51 / 58 25 29 99
info@mbconnectline.com
www.mbconnectline.com

Vulnerability SIM#2024-04-f:
"tmp directory exposed via webservice"

Details

CVE: CVE-2024-45276
Description: The mbNET.mini devices exposes its /tmp directory via the webserver and allows access to potentially sensitive files.
Solution: Update to latest version: 2.3.1

Affected Products

Product:	*Version:*	*Update:*
mbNET.mini	<= 2.2.13	2.3.1

CVSS Scores & Vulnerability

CWE-Identifier:	CWE-552
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#2024-04 / Rev.: 4
Created by:fade / 2024-10-21

Red Lion Europe GmbH
Winnettener Str. 6
91550 Dinkelsbühl
GERMANY

+49 (0) 98 51 / 58 25 29 0
+49 (0) 98 51 / 58 25 29 99
info@mbconnectline.com
www.mbconnectline.com