SIM#2020-02

Security Incident Management

Incident reported by:	*Date:*
CERT@VDE	02.04.2020
Referenced Documents:	
CVE-2020-8597	
Incidents covered by this document:	
• Vulnerability SIM#2020-02-a: "Buffer overflow in pppd"	

Public disclosure:	*Date:*
Incident-Report - SIM#2020-02	26.05.2020
mbNET/mbNET.rokey Firmware 6.2.3	09.04.2020
mbNET HW1 Firmware 5.1.10	30.04.2020
mbNET.mini Firmware 2.0.8	30.04.2020
mbSPIDER Firmware 2.6.5	08.05.2020
mymbCONNECT24 Firmware 2.6.1	16.07.2020

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#2020-02-a:
"Buffer overflow in pppd"

Details

CVE: CVE-2020-8597
Description: pppd (Point to Point Protocol Daemon) versions 2.4.2 through 2.4.8 are vulnerable to buffer overflow due to a flaw in Extensible Authentication Protocol (EAP) packet processing in eap_request and eap_response subroutines
Solution: **mbNET/mbNET.rokey, mbNET.mini and mbSPIDER:** Update to latest available Firmware. **mymbCONNECT24:** Update to latest available Firmware. **mbCONNECT24:** Not vulnerable.

Affected Products

Product:	*Version:*	*Update:*
mymbCONNECT24	<= 2.5.1	2.6.1
mbNET/mbNET.rokey	<= 6.2.2	6.2.3
mbNET HW1	<= 5.1.9	5.1.10
mbNET.mini	<= 2.0.6	2.0.8
mbSPIDER	<= 2.6.3	2.6.5

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

Document: SIM#2020-02 / Rev.: 25
Created by: fade / 2020-09-30