Security Incident Management

Incident reported by: ditis Systeme	***Date:*** 15.05.2023
Incident coordinated by: CERT@VDE	
Incidents covered by this document: ▪ Vulnerability SIM#2023-04-a: "Stored XSS in Diagnosis page"	
VDE-ID: VDE-2023-012	
Public disclosure:	***Date:***
Incident-Report - SIM#2023-04 mbNET/mbNET.rokey Firmware 7.3.2	17.08.2023 05.07.2023

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

Document: SIM#2023-04 / Rev.: 8
Created by:fade / 2023-08-17

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#2023-04-a:
"Stored XSS in Diagnosis page"

Details

CVE: CVE-2023-34412
Description: There exists a vulnerability in all mbNET/mbNET.rockey devices with firmware <= 7.3.1 that allows an authenticated attacker to store an arbitrary JavaScript payload on the diagnosis page of the device. That page is loaded immidiatly after login in to the device and runs the stored payload, allowing the attacker to fully compromise the browsing context. The payload is deleted on device reboot.
Solution: Update to latest version: 7.3.2

Affected Products

Product:	*Version:*	*Update:*
mbNET/mbNET.rokey	<= 7.3.1	7.3.2

CVSS Scores & Vulnerability

CWE-Identifier:	CWE-79
CVSS Base Score:	8.3
CVSS v3 Link:	AV:N/AC:L/PR:H/UI:R/S:C/C:H/I:H/A:L

Document: SIM#2023-04 / Rev.: 8
Created by:fade / 2023-08-17

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