Security Incident Management

Incident reported by: S. Dietz (CyberDanube Security Research)	***Date:*** 15.05.2024
Incident coordinated by: CERT@VDE	
Incidents covered by this document: ▪ Vulnerability SIM#2024-02-a: "Command injection"	
VDE-ID: VDE-2024-030	

Public disclosure:	***Date:***
Incident-Report - SIM#2023-04 mbNET.mini Firmware 2.2.13	03.07.2024 07.06.2024

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

Vulnerability SIM#2024-02-a: "Command injection"

Details

CVE: CVE-2024-5672
Description: There exists a vulnerability in all mbNET.mini devices with firmware <= 2.2.11 that allows a high privileged remote attacker to execute arbitrary system commands via GET requests due to improper neutralization of special elements used in an OS command.
Solution: Update to latest version: 2.2.13

Affected Products

Product:	***Version:***	***Update:***
mbNET.mini	<= 2.2.11	2.2.13

CVSS Scores & Vulnerability

CWE-Identifier:	CWE-78
CVSS Base Score:	7.2
CVSS v3 Link:	AV:N/AC:L/PR:H/UI:N/S:U/C:H/I:H/A:H

Document: SIM#2024-02 / Rev.: 5
Created by:fade / 2024-07-03