Security Incident Management

Incident reported by:	*Date:*
Noam Moshe @ Claroty	13.04.2021
Referenced Documents: claroty_report_210413.zip	
Incidents covered by this document: • Vulnerability SIM#2021-03-a: "Privilege escalation in mbConnect24serv" • Vulnerability SIM#2021-03-b: "RCE in mbConnect24serv"	
VDE-ID: VDE-2021-017	

Public disclosure:	*Date:*
Incident-Report - SIM#2021-03	22.07.2021
Update SIM#2021-03-b	28.03.2022
mbDIALUP V3.9R0.5	13.07.2021

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#2021-03-a:
"Privilege escalation in mbConnect24serv"

Details

CVE: CVE-2021-33526
Description: A low privileged local attacker can send a command to the service running with NT AUTHORITY\SYSTEM instructing it to execute a malicous OpenVPN configuration resulting in arbitrary code execution with the privileges of the service.
Solution: Update to version V3.9R0.5.

Affected Products

Product:	*Version:*	*Update:*
mbDIALUP	<= 3.9R0.0	3.9R0.5

CVSS Scores & Vulnerability

CWE-Identifier:	CWE-269
CVSS Base Score:	7.8
CVSS v3 Link:	AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H

Document: SIM#2021-03 / Rev.: 15
Created by:fade / 2022-03-28

Vulnerability SIM#2021-03-b: "RCE in mbConnect24serv"

Details

CVE: CVE-2021-33527
Description: ~~A low privileged local attacker can send a command to the service running with NT AUTHORITY\SYSTEM, that will not correctly validate the input, instructing it to execute arbitrary code with the privileges of the service.~~ **UPDATE 2022-03-28:** A remote attacker can send a specifically crafted HTTP request to the service running locally with NT AUTHORITY\SYSTEM, that will not correctly validate the input, instructing it to execute arbitrary code with the privileges of the service. There are some conditions that have to be met for this to work remotely that an attacker may not be able to control reliably.
Solution: Update to version V3.9R0.5.

Affected Products

Product:	*Version:*	*Update:*
mbDIALUP	<= 3.9R0.0	3.9R0.5

CVSS Scores & Vulnerability

CWE-Identifier:	CWE-78
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#2021-03 / Rev.: 15
Created by:fade / 2022-03-28