VERCOM

Summary of the Security Test

SCOPE

Summary of the *.messageflow.com web application security test

TEST DATA

05.12.2024 - 16.12.2024

SUMMARY DATE

24.01.2025

AUDITORS

Gilewicz Michał

Executive Summary

This document is a summary of work conducted by Michał Gilewicz. The subject of the test were the following web applications: *. messageflow.com i.e app.messageflow.com and appbackend.messageflow.com including panels of the Emaillabs, Redlink and MessageFlow brands.

The main focus of the test is to obtain vulnerabilities that have or may have a negative impact on the confidentiality, integrity and availability of the processed data.

Security tests were carried out in accordance with commonly accepted methodologies for testing web applications, such as: OWASP TOP10 or OWASP ASVS, which included, inter alia, tests aimed at finding errors related to the possibility of malicious code injection (XSS, SQLi, SSTI, etc.), errors related to authentication or related to incorrect server configuration. In addition, during the audit, the infrastructure was scanned in order to find vulnerable software / libraries, as well as open ports that could have an impact on network security.

The audit used an approach based on manual tests based on the above-mentioned methodologies, and supporting these activities with a number of automated tools, including:Burp Suite Professional, Dirbuster, Nessus Professional, Nmap, sqlmap, ffuf.

It has been confirmed that all security errors found during the security audit have been corrected and there is no further possibility of their use by third parties.