Executive Summary

Artemis Gas, Inc.

This document is an executive summary of the report of the findings of a security assessment performed on ARTEMIS GAS, INC. (“Artemis”). A full version of this report is available as the Detailed Technical Report submitted alongside this document. This assessment was performed as an external penetration test. The primary objective of this security assessment was to find any potential vulnerabilities or other avenues for exploit in Artemis’ computer systems/networks, and to provide recommendations on how the company can improve its security posture. The primary assumption made before performing this security assessment was that the networks and web servers were in some way accessible to the testers in order to be able to scan for vulnerabilities and test exploits, whether by already being public networks or by being provided special access for the purposes of completing the test. The penetration test began on September 10, 2023, and end on September 24, 2023, lasting 2 weeks in total.

Summary of Findings

There were nine main vulnerabilities uncovered over the course of this assessment, of varying degrees of severity. The chart below shows the breakdown of the severity classes of the vulnerabilities that were discovered. Some of the vulnerabilities may vary in severity depending on context, so the “Low Estimate” column corresponds to the best-case scenario and the “High Estimate” column corresponds to the worst-case scenario.

Severity	Risks (Low Estimate)	Risks (High Estimate)
none	0	0
low	0	0
medium	1	0
high	4	2
critical	4	7

Recommendations

Keep things patched and up-to-date. Several of the vulnerabilities discovered are already well documented and patches exist that solve the issue, so these should be installed as soon as possible. More generally, implement a policy of regularly checking for security updates and patches for the software (and hardware/firmware) being used and installing them in a timely manner. Additionally, ensure the company has clear security policies based in best practices surrounding technology use and maintenance, and ensure these policies are known, understood, and followed. Refer to the full detailed technical report for item-specific recommendations.