EXECUTIVE SUMMARY

Artemis Gas Inc. was provided with a vulnerability assessment led by Nguyen La - a Cybersecurity Analyst at our firm. The assessment was conducted in January 2024. The purpose of this assessment was to identify the risk posture of Artemis, which includes vulnerabilities in its systems and networks, the threats that Artemis has to face, as well as the recommendations on how to remediate these vulnerabilities.

We identified a total of 9 vulnerabilities in the Artemis's network, ranging from Critical to Medium in terms of severity. Specifically, there are 1 Critical-risk vulnerability, 6 High-risk vulnerabilities and 2 Medium-risk vulnerabilities. **Our company recommends the remediations must be done within the next 30 days in order to mitigate the risk of cyber attacks upon Artemis's network.**

KEY SUMMARY OF FINDINGS AND RECOMMENDATIONS:

Our company ranked the severity of each risk based on CVSS score - an indicator of how severe the vulnerabilities are. Below is the top 2 highest CVSS score along with remediation methods:

1. **Web Application Vulnerable to SQL Injection:** Attackers can manipulate SQL queries through user inputs, potentially gaining unauthorized access to the database. This could lead to data theft, unauthorized access to sensitive information, and potential manipulation of the application's database.
   Remediation: Artemis should implement input validation and parameterized queries to prevent SQL injection attacks, as well as regularly conduct code reviews and security assessments of the web application.
2. **Apache Web Server Vulnerable to CVE-2019-0211:** This specific vulnerability allows remote code execution. This would enable remote attackers to exploit this vulnerability, then execute arbitrary code on the server, leading to potential system compromise.
   Remediation: Artemis should apply the latest patches and updates for Apache to address the CVE-2019-0211 vulnerability and consider configuring web application firewall (WAF) to detect and block potential exploits.

CONCLUSION

This vulnerability assessment has shown that Artemis has to immediately address these gaps in their network **within the next 30 days** in order to mitigate the risk of cyber attacks, especially the vulnerabilities ranked as Critical-risk and High-risk.

The full list of vulnerabilities will be attached below. Further details on risk ratings and remediation methods can be found on **Detailed Technical Report**.

Number	Vulnerability	CVSS score	Threat Level
1	Unpatched RDP Exposed to the Internet	8.2	**High**
2	Web Application Vulnerable to SQL Injection	9.0	**Critical**
3	Default password on Cisco admin portal	6.9	**Medium**
4	Apache web server vulnerable to CVE-2019-0211	8.8	**High**
5	Web server is exposing sensitive data	7.5	**High**
6	Web application has broken access control	8.2	**High**
7	Oracle WebLogic Server vulnerable to CVE-2020-14882	8.2	**High**
8	Misconfigured cloud storage (AWS security group misconfiguration, lack of access restrictions)	7.1	**High**
9	Microsoft Exchange Server vulnerable to CVE-2021-26855	6.5	**Medium**

Table 1. Risk Analysis Using CVSS Score

Low	**0.1 - 3.9**
Medium	**4.0 - 6.9**
High	**7.0 - 8.9**
Critical	**9.0 - 10.0**

Table 2. CVSS Qualitative Values