**Name: Tanvir Ahmed**

**CONFIDENTIAL Artemis Inc**

**Vulnerability Assessment**

**EXECUTIVE SUMMARY**

Artemis, a natural gas corporation serving 1.7 million customers, has commissioned a cybersecurity firm to conduct a vulnerability assessment to determine the risk and internal and external threats that may arise in the company. The assessment took place in June 2025. The firm thoroughly assessed Artemis’s Web applications, network infrastructure and cloud services. This report provides a summary of the overall findings and analysis of all identified vulnerabilities, along with detailed recommendations for high risk issues.

The assessment revealed that Artemis has major flaws in its web application that jeopardize the company’s data, business secrets, and sensitive customer information attracting attackers who can exfiltrate data and move laterally within the network. The film has identified 5 critical and 4 high risk vulnerabilities in the Artemis network. The firm recommends immediately patching the critical risk before any major damages occur.

Key Summary Findings and Recommendations

1. Four outdated and unpatched services exist in the internal network. Leaving such crucial services vulnerable can expose Artemis to significant risks, potentially resulting in large data leaks and full system compromise.

**FRM RECOMMENDATION**

The firm recommends patching these services and updating the software immediately, followed by a reevaluation of the overall security posture. A dedicated team should be assigned to recalibrate the softwares if a remediation team is not already in place. These vulnerabilities must be fixed, and a new policy should be implemented to regularly check for such issues and maintain in the highest security standards and procedures.

1. There are misconfigurations in web applications and cloud systems that must be addressed. These vulnerabilities could lead to major attacks on the Apollo system, exposing business secrets and other sensitive information.

**FIRM RECOMMENDATIONS**

A new policy should be established to introduce stronger hardening techniques and address vulnerabilities in the network and web applications. The IT team should properly configure these services, update security measures, and improve cloud systems to eliminate flaws that could result in major data leak.

**CONCLUSION**

The Assessment has shown that Artemis has many vulnerabilities and unpatch programs that must be addressed. More importantly, new policies need to be established to focus more on improving network and web application security. Without updated policies and proper security measures, vulnerability will continue to exist and provide opportunities for exploitation.

Artemis should invest in a qualified security team to improve vulnerability management and continuously monitor for unpatched critical and high risks services. Critical vulnerabilities should be fixed within 30 days to reduce the chance of major security breaches.