**Artemis Inc.**

**Penetration Test Conducted by Long Trang Corp.**

**EXECUTIVE SUMMARY**

Artemis Inc engaged Long Trang Corp. to conduct a penetration testing on their network infrastructure to assess the risk of potential security threats. The test was done on March 22, 2023. Long Trang Corp. performed an external network vulnerability assessment from the security analyst’s host from the internet and an internal network vulnerability assessment from the security analyst’s laptop wired to Artemis’s internal corporate network. This report provides a summary of the overall findings and displays statistical charts for all detected vulnerabilities. Recommendations will be addressed for the critical and high-risk vulnerabilities.

The assessment results indicate that Artemis Inc. will be vulnerable to attacks from both external and internal threat actors unless it addresses the following:

* Improve patch management procedures for critical updates to the operating system and services
* Put proper security controls in place for new network devices
* Implement security controls during the software development life to address code injection vulnerabilities

**CONCLUSION**

The penetration testing conducted by our security firm on Artemis Inc's network infrastructure revealed that the organization may have process gaps in its patch and vulnerability management practices, potentially exposing it to threats from internal and external sources. The test identified 4 **critical**-risk, 3 **high**-risk, and 2 **medium**-risk vulnerabilities on the internal network. We advise remediation of the critical and high-risk vulnerabilities within 30 days to mitigate the risk of network exposure to attacks. Artemis Inc. should adopt a proactive approach to address security vulnerabilities, going beyond the necessary steps for remediation. This entails providing regular training to its staff, collaborating with external security vendors, and consistently conducting research on emerging security threats.