Executive Summary

Artemis, Inc. Vulnerability Assessment Summary

Objective: Artemis, Inc. engaged [Your Company Name] to conduct an external vulnerability assessment to identify potential security risks within its network. This assessment focused on examining the risks posed by various vulnerabilities, particularly those that could expose Artemis to unauthorized access, data breaches, or operational disruptions. The assessment results are presented here for senior management review, highlighting the primary risks, business impact, and recommended mitigations to address critical security threats.

Key Findings and Business Impact

Our assessment of Artemis's infrastructure identified several key vulnerabilities with varying degrees of risk. The highest-priority issues, marked in red and orange, require immediate attention to reduce exposure to potential security breaches. This report summarizes our findings and provides actionable recommendations for reducing risk.

1. Exposed Remote Desktop Protocol (RDP)

- **Risk Level**: Critical
- **Business Impact**: Unauthorized access through RDP can enable attackers to control network resources, leading to data breaches or service disruptions.
- **Recommendation**: Limit RDP access to internal networks only, and ensure that all instances are patched and monitored.

2. Web Application Vulnerable to SQL Injection

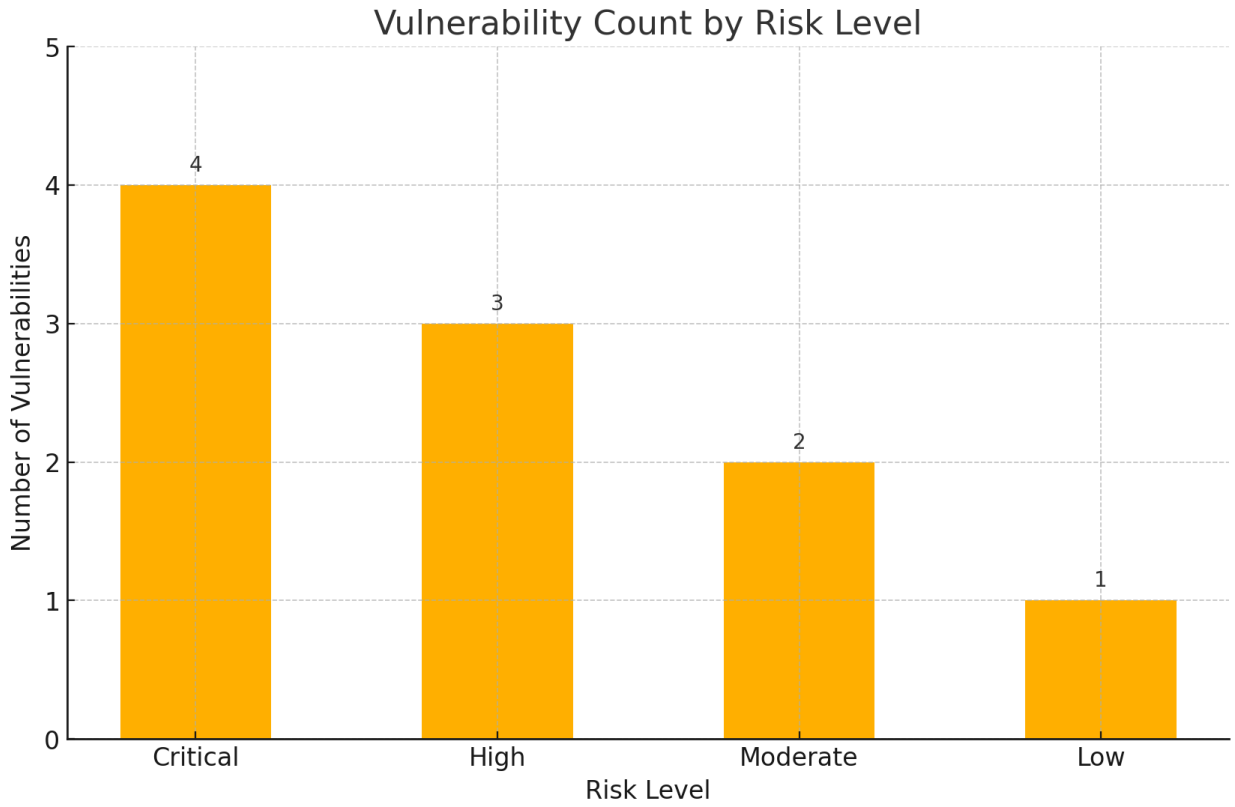
- **Risk Level**: High
- **Business Impact**: Allows potential access to sensitive customer and corporate data, risking data integrity and customer privacy.
- **Recommendation**: Implement parameterized queries and a Web Application Firewall (WAF) to mitigate SQL injection risks.

3. Unsecured Cloud Storage (AWS S3 Misconfiguration)

- **Risk Level**: High
- **Business Impact**: Potential exposure of sensitive data, including client information and intellectual property, due to unrestricted access permissions.
- **Recommendation**: Configure access policies to apply strict permissions, restricting access to only authorized personnel.

Risk Distribution and Prioritization

The chart below illustrates the distribution of vulnerabilities identified by risk severity. Addressing critical and high-risk vulnerabilities is a priority to safeguard sensitive data and maintain operational integrity.



Conclusion

The findings of this assessment indicate that Artemis's current security posture can be significantly improved by addressing identified vulnerabilities in a structured and prioritized manner. Immediate attention to critical issues will reduce the risk of unauthorized access and protect Artemis's critical assets. Our team is available to support Artemis in implementing these recommendations to ensure a robust and resilient security framework.