Detailed Technical Report

A. Cover Page

Artemis, Inc. External Vulnerability Assessment
Conducted by: The Consultants
Date: Oct 31, 2024

B. Table of Contents

C. Scope of Work

This assessment focused on external-facing services and infrastructure, including web applications, cloud storage configurations, and network protocols that could be exploited by threat actors. The goal was to identify vulnerabilities that might allow unauthorized access or data compromise.

D. Project Objectives

1. Identify potential security vulnerabilities in Artemis's network.
2. Evaluate the risks posed by these vulnerabilities to Artemis’s business operations.
3. Provide actionable recommendations to mitigate identified risks.

E. Assumptions

- All systems were accessible for testing, with permissions granted for simulated attack scenarios.
- Scanning and vulnerability assessments were performed under a controlled, ethical testing environment.

F. Timeline

Phase	Date Started	Date Completed
Reconnaissance	Oct 15	Oct 17
Network Scanning	Oct 18	Oct 22
Vulnerability Analysis	Oct 23	Oct 28
Reporting	Oct 29	Oct 30

G. Summary of Findings

Vulnerability	Description	Risk Level	Potential Impact
Exposed RDP	Unpatched RDP accessible externally	Critical	Unauthorized remote access, potential for DoS attacks
SQL Injection	Injection vulnerability in web application	High	Data exposure, potential for unauthorized data alteration
AWS S3 Misconfiguration	Public access to sensitive data due to incorrect permissions	High	Data leakage, exposure of sensitive information
Apache CVE-2019-0211	Privilege escalation vulnerability in Apache HTTP Server	High	Unauthorized control of server, potential lateral movement
Default Cisco Admin Credentials	Default password on Cisco admin portal	Moderate	Unauthorized configuration changes, network disruption

H. Recommendations

1. Restrict RDP Access

- **Recommendation**: Disable external access to RDP or restrict to a virtual private network (VPN) only. Apply latest patches to all RDP services.
- **Impact**: Reduces risk of unauthorized remote access, protecting internal network resources.

2. SQL Injection Mitigation

- **Recommendation**: Implement parameterized queries and input validation on web application forms. Install a WAF with SQL Injection protection enabled.
- **Impact**: Safeguards sensitive information and mitigates risk of data corruption from malicious SQL queries.

3. AWS S3 Configuration Review

- **Recommendation**: Review and apply strict IAM permissions for S3 buckets to enforce least privilege. Disable public access settings.
- **Impact**: Prevents exposure of sensitive information by ensuring only authorized users have access.

4. Apache Web Server Security Patches

- **Recommendation**: Update Apache servers to the latest version, CVE-2019-0211 patched.
- **Impact**: Prevents privilege escalation risks, securing the server against unauthorized access.

5. Enforce Strong Password Policies

- **Recommendation**: Ensure default passwords are changed across all network devices, particularly Cisco equipment. Enforce a strong password policy with 2FA for added security.
- **Impact**: Protects network devices from unauthorized access and reduces attack surface.

Appendices

Appendix A: Reconnaissance Activities

Methodology: Utilized passive information-gathering techniques and tools such as Shodan, DNS enumeration, and OSINT (Open Source Intelligence) to identify public-facing infrastructure and potential entry points.

Appendix B: Network Scanning and Enumeration

Tools Used:

- **Nmap**: Identified open ports and services across external IP addresses.
- **OpenVAS**: Scanned for network-layer vulnerabilities.

Appendix C: Detailed Vulnerability Analysis

1. **Exposed RDP (CVE-2019-0708)**
    - **Description**: Unpatched RDP accessible externally.
    - **Impact**: High risk of unauthorized access.
    - **Remediation**: Apply patch and restrict RDP to internal network.
2. **SQL Injection**
    - **Description**: SQL injection found on critical application input fields.
    - **Impact**: High risk of unauthorized data access.
    - **Remediation**: Implement prepared statements and input validation.

Conclusion

This detailed technical assessment reveals a set of critical and high-risk vulnerabilities that, if exploited, could pose significant security threats to Artemis. To ensure Artemis's resilience against such risks, we recommend prioritizing the immediate remediation of exposed RDP, SQL Injection vulnerabilities, and AWS S3 misconfigurations, followed by patching vulnerable software and enforcing strong password policies.

Our team is available to provide further assistance in implementing these recommendations. With timely action, Artemis can establish a more secure and resilient environment against emerging cyber threats.