Detailed Technical Report

Penetration Testers R US

For Artemis Inc.

V1.0

June 1st, 2022

By: Zackery Valete Rodriguez

Table of Contents

1. Executive Summary

CONFIDENTIAL Artemis Inc.

Vulnerability Assessment

Artemis Inc. engaged Penetration Testers R US to provide a vulnerability assessment (“Assessment”) to determine the risk of compromise due to internal or external threats. The assessment was conducted on { testing date here }.

Penetration Testers R US performed an external network-layer vulnerability assessment on Artemis Inc.’s cloud and on premises networks from a Penetration Testers R US host on the internet. The results from said assessment have been summarized to highlight all findings and statistics for all identified vulnerabilities found within the time constraints, as well as the detailed findings and recommendations needed to remedy these vulnerabilities.

The findings indicate that Artemis Inc. has clear process gaps in its patch, configuration, and vulnerability management processes, all of which leave the organization vulnerable to attacks from both internal and external sources. Penetration Testers R US identified 3 medium-risk, 4 high-risk, and 2 critical-risk vulnerabilities on the internal network and external networks. Penetration Testers R US recommends remediation of the critical-risk and high-risk vulnerabilities within the next 30 days to reduce the risk of exposing the network to attacks. Moreover, due to the types of vulnerabilities found, it is highly recommended for Artemis Inc. to schedule a more in depth vulnerability assessment to look for vulnerabilities that require sophistication.

Key Summary Findings and Recommendations:

- Broken Access Controls
    a. Review and test access controls to ensure users can only access and perform actions based on the principle of least privilege.
- Patching required for multiple systems
    a. Verify compatibility with the latest stable versions for each outdated system and apply as soon as possible.
- Weak system configurations
    a. Review manuals, contact vendors, and seek certifications to ensure that systems are configured properly.
- Weak web application security
    a. Review manuals, contact vendors, and seek certifications to ensure that web applications are built and maintained with security in mind.
- Weak encryption standards
    a. Conduct testing and balance speed with security when using the latest available and compatible encryption security suites.

Conclusion:

The Assessment has shown that while Artemis Inc. has a fully functioning and capable cloud and on premise networks, the current standing of the security for these networks are not sufficiently effective to mitigate risk. These unmitigated vulnerabilities, if exploited by an attacker, can be used to potentially compromise the full Artemis Inc. network (including both the cloud and on prem networks).

Artemis Inc. should investigate opportunities to keep up with modern-day best practices and to promote the value and importance that cybersecurity entails.

2. Scope of Work

A current network diagram was not provided by Artemis Inc. As such, this vulnerability assessment covers the external penetration testing of all Artemis Inc.'s cloud and on premise assets that we were able to locate within the time allotted.

Time restrictions provided by Artemis Inc. have been taken into account to ensure all parties are aware that thorough review of all possible vulnerabilities within the time allotted will not be possible.

The approach to be taken, client's concerns, and client's expectations have been reviewed and approved by Artemis Inc. prior to the start of testing.

2.1 Project Objectives

This vulnerability assessment is carried out to determine the security posture of the assets found within Artemis Inc.'s cloud and on prem networks. The results and findings from the assessment are used to confirm the vulnerabilities found. With the agreed upon time allotted, only immediately exploitable services have been tested. Risk ratings based on threat, vulnerability, and impact have been provided.

2.2 Assumptions

While performing the vulnerability assessment, due to the inability to provide the network diagrams for both the cloud and on premises networks; it has been noted and approved by Artemis Inc. that take downs, disruptions, and other possible negative outcomes may arise throughout the assessment. Furthermore, the NDA and rules of engagements including the above have been signed.

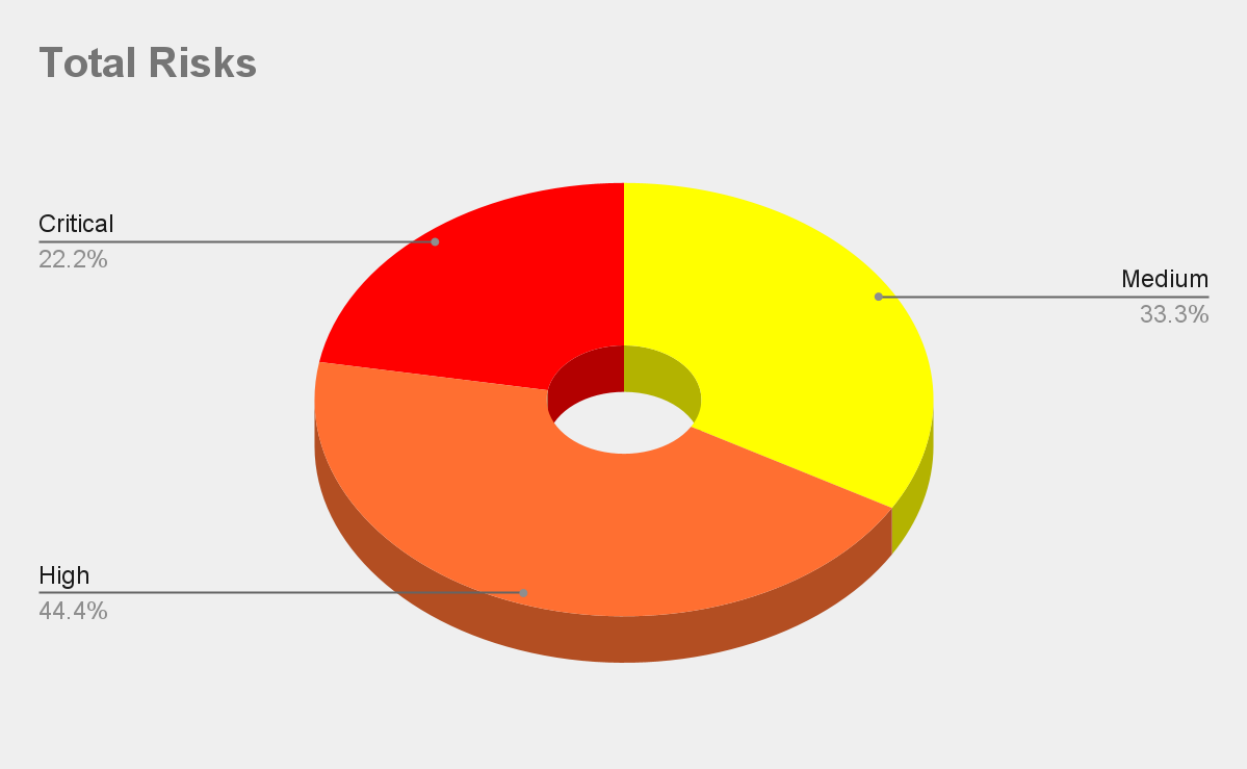
2.3 Timeline

The timeline of the test is as below:

Penetration Testing	Start Date/Time	End Date/Time
Pen Test 1	mm/dd/yyyy	mm/dd/yyyy

3. Summary of Findings

Value	Number of Risks
Low	0
Medium	3
High	4
Critical	2



It is highly recommended for Artemis Inc. to review this assessment and quickly align their networks to the best practices provided as soon as possible. This is due to the issue that we were able to exploit critical vulnerabilities such as access to the Cisco admin portal in less than an hour. Vulnerabilities that lead to full takeovers like the above can be devastating for Artemis Inc. . Losses are not limited to financial damages in these cases and easily will involve compliance failures as well as immediate and permanent loss of Artemis Inc.’s clients and reputation. Even with a defense-in-depth approach, having easy to access doors such as the above will lead to virtually guaranteed data breaches.

In addition to the hardening of the networks and the securing of the current configurations, it is also recommended that the current security professionals maintaining Artemis Inc. 's networks should gain and/or recertify with the certifications provided from organizations such as CompTIA and AWS. We at Penetration Testers R US are always happy to find sophisticated and hard to find vulnerabilities to prove and drive our value within the

market, but the findings we've come across today are of bare minimum cybersecurity knowledge requirements and this needs to be remedied as soon as possible.

Below are the high level findings each with their assigned risks and conclusions from the external penetration test:

- Unpatched RDP is exposed to the internet
    - Risks of what a threat actor can accomplish:
        - Gaining access to a user's workstation (possibly high level)
        - Downloading and installing backdoors and malware to achieve persistence
        - Breaching of all information accessible by the user (due to access control failures, possibly many if not all users)
        - Gain a strong foothold to begin privilege escalation
    - Conclusion:
        - It is important to note that with the existence of this finding, that a threat actor would not need much time or expertise to exploit this vulnerability and that the end result could be catastrophic when combined with the other vulnerabilities seen below.
- Web application is vulnerable to SQL Injection
    - Risks of what a threat actor can accomplish:
        - Unauthorized viewing of tables, views, and the entire database
        - Deletion/alteration of entire tables/databases
        - The attacker could gain administrative rights to a database which can open more footholds into the network.
    - Conclusion:

        - Compliance and full application failures could occur depending on the type and success of the SQL injection that is used by an attacker.
- Default password on Cisco admin portal
    - Risks of what a threat actor can accomplish:
        - The attacker could gain full access to the portal to change, update, download copies, and delete anything they'd like
        - The attacker could eavesdrop on the portal, siphoning data/information the entire time until they are spotted and stopped.
    - Conclusion:
        - This vulnerability would give an attacker a baseline of Artemis Inc. 's network security that would motivate them to dig more deeply into the company’s networks since very little skill may be required to breach the other areas of Artemis Inc. ‘s network.
- Apache web server vulnerable to CVE-2019-0211
    - Risks of what a threat actor can accomplish:
        - Gain the ability to execute arbitrary code with the privileges of the parent process (usually root) by manipulating the scoreboard
    - Conclusion:
        - A threat actor with the ability to execute arbitrary code is one of the worst case scenarios for any network. This will allow installation of malware, backdoors, eavesdropping software, and more that may be very difficult to find/remedy even after the remediation of this vulnerability.
- Web server is exposing sensitive data
    - Risks of what a threat actor can accomplish:
        - Exposed data can be recorded by the attacker
        - Failure with compliance

        - Loss of clientele
    - Conclusion:
        - Sensitive data exposure can lead to not only fines, but the loss of trust of those involved with the sensitive data in question.
- Web application has broken access control
    - Risks of what a threat actor can accomplish:
        - If an attacker gains access to a user's account (even low level), the attacker may be able to execute actions of a similar yet different level or worse, a higher level account than its own.
    - Conclusion:
        - While broken access control opens many doors for external attackers, it's important to note that it also opens many doors for internal threat actors as well as accidental damages from regular users.
- Oracle WebLogic Server vulnerable to CVE-2020-14882
    - Risks of what a threat actor can accomplish:
        - Allows unauthenticated attackers with network access via HTTP to compromise Oracle WebLogic Server.
        - Successful attacks of this vulnerability can result in takeover of Oracle WebLogic Server.
    - Conclusion:
        - This critical vulnerability "hands the keys" of the server, so to speak, to any attacker willing to attempt this extremely easy to exploit vulnerability.
- Misconfigured cloud storage (AWS security group misconfiguration, lack of access restrictions)
    - Risks of what a threat actor can accomplish:

        - Ease of accessing privileged actions and information with a compromised account.
    - Conclusion:
        - If an attacker gains a foothold into the cloud, this vulnerability will make it much easier to escalate privilege and access information that is normally harder to reach.
- Microsoft Exchange Server vulnerable to CVE-2021-26855
    - Risks of what a threat actor can accomplish:
        - Allow an attacker to remotely execute malicious code on a computer.
        - Code executed, could steal or alter information or alter the infrastructure within or connected to the server.
    - Conclusion:
        - Similar to the Apache web server vulnerability, this vulnerability will allow installation of malware, backdoors, eavesdropping software, and more that may be very difficult to find/remedy even after the remediation of this vulnerability.

4. Recommendations

- Unpatched RDP is exposed to the internet
    - Recommendation:
        - Verify compatibility with the needed patch and apply immediately.
- Web application is vulnerable to SQL Injection
    - Recommendation:
        - White list inputs
        - Black list inputs

        - Input validation
        - Parameterized queries including prepared statements
        - Automate vulnerability testing with tools such as SQLmap
- Default password on Cisco admin portal
    - Recommendation:
        - Update admin portal with a strong password.
        - Conduct thorough testing of the portal to confirm no persistence of an ongoing attack.
- Apache web server vulnerable to CVE-2019-0211
    - Recommendation:
        - Review compatibility of attached services/processes and update the server to the latest stable version as soon as possible.
        - Verify that the principle of least privilege is strict
- Web server is exposing sensitive data
    - Recommendation:
        - Secure the data with strong and up to date encryption and hashing suites
        - Clarify specifically why the data is being exposed and correct the issue
- Web application has broken access control
    - Recommendation:
        - Review best practices for access control
        - Automate access control
        - Set alerts for access control
- Oracle WebLogic Server vulnerable to CVE-2020-14882
    - Recommendation:

        - Verify compatibility and update the server to the latest stable version as soon as possible
- Misconfigured cloud storage (AWS security group misconfiguration, lack of access restrictions)
    - Recommendation:
        - Reconfigure and regularly test the configurations to make sure they work as intended
        - Ensure users/admins are up to date with aws certifications and aws best practices
- Microsoft Exchange Server vulnerable to CVE-2021-26855
    - Recommendation:
        - Update the server to the latest stable version as soon as possible