Phase 5.1

Detailed Technical Report

Phase 5: Final Reports

Artemis INC.
Vulnerability Assessment

Detailed Technical Report

Artemis INC Vulnerability Assessment Report

For Artemis INC.

Version 1.0

January 5th, 2023

By Jeff Tsui

Document Properties

Title	Artemis INC Vulnerability Assessment Report
Version	V1.0
Author	Jeff Tsui
Pen-tester	Jeff Tsui
Reviewed By	Lee Campbell
Approved By	Lee Campbell
Classification	Confidential

Version Control

Version	Date	Author	Description
Version 1.0	January 5th, 2023	Jeff Tsui	Final Draft

Table of Contents

A. Scope of Work

This vulnerability assessment will consist of using scanning tools such as Nmap, Acunetix, OpenVAS, and Burp Suite to run scans and identify vulnerabilities. This assessment aimed to provide an overview of the level of security on Artemis's internet infrastructure, such as network and web applications. Also, identify any potential weaknesses within its internet infrastructure.

B. Project Objectives

This vulnerability assessment determines the security posture of Artemis's internet infrastructure. The assessment outcome will be analyzed for potential vulnerabilities that can damage the Artemis company and its security system. A risk rating is assigned to each vulnerability based on the threat level, vulnerability, and impact on the company.

C. Assumptions

Some of Artemis's data centers use older network hardware that may be outdated from support and vulnerable to unpatched issues. Other data centers have newer network hardware but may not be configured properly and may also be vulnerable to attacks. Some policies for storing data in the cloud and creating websites may not be configurated properly. Also, improper management for the admins and employees may lead to vulnerabilities that can expose the network to unknown risks.

D. Timeline

Timeline of the vulnerability assessment is as below:

Penetration Testing	Start Date	End Date
Test 1	01/05/2023	01/26/2023

Table 1: Penetration Testing Timeline

E. Summary of Findings

Risk Type	Number of Risks
High	1
Critical	6

Table 2: Total Risk Rating

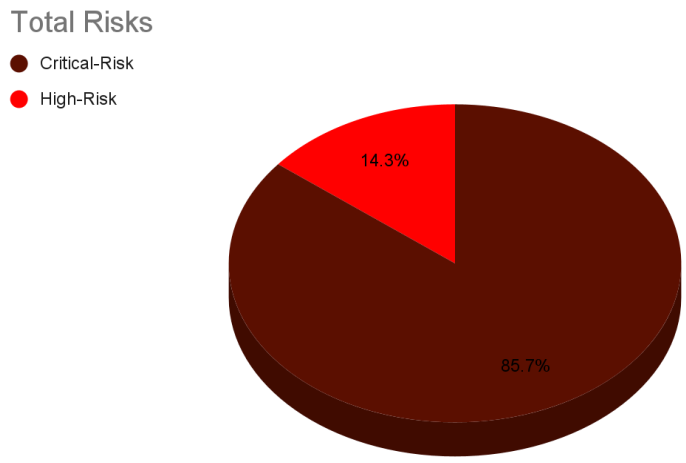

Figure 1: Total Risks Percentage

1. **Unpatched RDP is Exposed to the Internet**:

   During the assessment, it was noticed that Cairo and Singapore's data centers use older network hardware than the other two sites. When using Nmap to scan for open ports, port 3389 was identified to be open, and the port is used for RDP. Further inspection of the RDP, it is unpatched and exposed to the internet, which is vulnerable to brute force attacks to gain access to the RDP. Leaving potential risks such as information disclosure to full system compromise. This vulnerability is similar to a successful attack in 2019, the Bluekeep attack (CVE-2019-0708).

- CVSS v3.0 Base Score - 9.8 **CRITICAL**
- CVSS Vector - CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C

2. **The Web Application is Vulnerable to SQL Injection**:

During the assessment of Artemis's main website login page, it is found vulnerable to SQL injection attacks using Acunetix's Cross-site scripting vulnerabilities scan. The attack can be done by inputting (admin' OR '1' = '1) as the username. Then anything for the password, anyone can bypass the authentication and authorization system and log in as the admin. The consequences of a successful SQLi attack cause loss of confidentiality since a company's SQL database typically holds sensitive information. Moreover, much information in the database can be modified or deleted, which can cause much damage to a company's integrity. This vulnerability is similar to the CVE-2022-1731.

- CVSS v3.0 Base Score - 9.8 **CRITICAL**
- CVSS Vector - CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

3. **Using Default Passwords on Newer Equipment (Fortinet):**

During the assessment of Artemis's hardware equipment, newer devices like Fortinet that are not configured properly were found using Burp Suite's intruder tool. Fortinet is using default credentials to log in to their admin portal. This default login information can usually be found on the product's official website or manuals. Hackers can use this information to gain access to the Fortinet devices and have full control of root or administrative privileges. This vulnerability is similar to the CVE-2020-3446.

- CVSS v3.0 Base Score - 9.8 **CRITICAL**
- CVSS Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

4. **The Web Server is Exposing Sensitive Data:**

During the assessment of Artemis's main website, sensitive data exposure resulting from a lack of encrypted protection was found using Burp Suite's automated scan. All sorts of data, ranging from authentication credentials, confidential business plans, and databases, can be stolen by attackers exploiting the weak encryption web server. Attacks such as SQL injection attacks, broken access control attacks, ransomware attacks, and insider threat attacks are all possible against a weak encryption web server.

- CVSS v3.0 Score: 9.4 **CRITICAL**
- CVSS v3.0 Rating: CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:L

5. **Vulnerability Found in an Unpatched Oracle WebLogic Server:**

During the assessment, an unpatched version 12.2.1.4.0 was found using the Oracle WebLogic Server. This version is vulnerable to a remote code execution vulnerability in the Oracle WebLogic Server of Oracle Fusion Middleware. This vulnerability can bypass the authentication and allows unauthorized hackers with HTTP network access to compromise the Oracle WebLogic Server completely. The exploit can be done with a single HTTP GET request. This vulnerability is similar to the CVE-2020-14882.

- CVSS v3.1 Score: 9.8 **CRITICAL**
- CVSS v3.1 Rating: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

6. **Misconfigured Security Group Policy on AWS Cloud Storage:**

During the assessment, misconfigured security group policy was found on AWS cloud storage allowing ports 22 and 3389 to have unrestricted access. Security groups should not allow port 22 traffic from or to the public internet because it is the secure shell port, a way for hackers to control an instance or a server remotely. Port 3389 is the Remote Desktop Protocol (RDP) port. This port should not allow traffic from or to the public internet either. Doing so might result in allowing hackers to compromise the RDP application, and they might potentially gain access to the organization's cloud-based data.

- CVSS v3.1 Score: 7.5 HIGH
- CVSS v3.1 Rating: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N

7. Vulnerability Found in an Unpatched Microsoft Exchange Server:

During the assessment, an unpatched 2019 version was found using Microsoft Exchange Server. This unpatched version of Microsoft Exchange is vulnerable to a server-side request forgery (SSRF) vulnerability. This vulnerability exploits and bypasses the authentication. Allowing sensitive information to leak onto the internal network, enabling hackers to download user emails and gain full access to the mail server. This vulnerability is similar to the CVE-2021-26855.

- CVSS v3.1 Score: 9.1 **CRITICAL**
- CVSS v3.1 Rating: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

F. RECOMMENDATION/ REMEDIATION ACTION

1. Unpatched RDP is Exposed to the Internet:

- Disable RDP if it is not needed.
- Use a stronger password for the machine.
- Close down port 3389 with a firewall

- Have a better antivirus system that features Remote Access Shield, such as the Avast Premium Security.

2. The Web Application is Vulnerable to SQL Injection:

- Use of prepared statements with parameterized queries.
    - All the SQL codes are defined and passed in each parameter. Therefore the attacker will not be able to change the query's intent.
- Use allowlist input validation.
    - Prevents unvalidated user input from being added to a query.
- Escape all user input.
    - A technique that escapes all user input. So the input is not confused with SQL code.
- Use of properly stored procedures.
    - Developers build SQL statements with parameters stored in the database only.

3. Using Default Passwords on Newer Equipment (Fortinet):

- Change the default password into a unique password.
- Use alternative authentication mechanisms like multi-factor authentication.
- Restrict network access to the devices,

4. The Web Server is Exposing Sensitive Data:

- Encrypt all sensitive data at rest.
- Classify all data and apply control to that data.
- Store passwords using a strong and salted hashing function.
- Use strong ciphers on the web servers.
- Do not store sensitive data after it is used.
- Disable caching for the response that stores sensitive data.

5. Vulnerability Found in an Unpatched Oracle WebLogic Server:

- Install the critical patch update released in October 2020.

6. **Misconfigured Security Group Policy on AWS Cloud Storage:**
   Only allowing specific IP addresses access to the secure shell port and RDP port.

- Log in to the AWS Console and navigate to Instances services.
- Click on the instance you want to modify its security group.
- Navigate to the security tab and click on the security groups above inbound rules.
- Click on inbound edit rules and look for SSH and RDP, change the source to “My IP,” or input the IP address range you want the security group to have access to.

7. **Vulnerability Found in an Unpatched Microsoft Exchange Server:**

- Install the mandatory patches for the affected version.
- Place the Exchange Server inside a VPN to separate port 443 from external connection requests.

G. CONCLUSION/ REMEDIATION ACTION

The Vulnerability assessment has shown that Artemis can patch and remediate the vulnerabilities. But these recommendations may not be comprehensive or sufficiently effective to mitigate all the risks. The vulnerabilities that are not mitigated can cause full company network compromise if exploited by an attacker.

Artemis INC. should investigate opportunities to improve its vulnerabilities and patch hardware and software applications recommended to ensure that all critical and high-risk vulnerabilities are dealt with within 30 days or less.