03/19/2023
Created by Cheyenne Rohrer

Executive Summary

Fictional Cyber Firm Inc. engaged ARTEMIS GAS INC. to provide a vulnerability assessment to discover risks caused by potential external or internal threats. This assessment was conducted in March of 2023. Fictional Cyber Firm Inc. performed an external vulnerability assessment which was conducted from a vendor host on the internet. The purpose of this assessment was to perform a penetration test/structured walkthrough of Artemis Gas, INC.'s technical setup and work products to find errors and improve the quality of their product and deliverable service.

The assessment results indicate that ARTEMIS GAS INC. has gaps in its vulnerability and patch management procedures which leaves the company vulnerable to attacks. Fictional Cyber Firm Inc. has identified 4 critical, 3 high, 1 medium, and 1 low risk vulnerabilities on the internal and external network. **Cyber Firm Inc. suggests remediation of the critical and high risk vulnerabilities within the next 14 days to reduce the risk of attack exposures.**

Key Summary Findings and Recommendations:

1. The ARTEMIS GAS INC. web application is vulnerable to SQL injections and unpatched RDP is exposed to the internet.

Cyber Firm Inc. Recommendations

- ➔ Use an RDP gateway server, reject requests from port 3389, enforce a remote access policy, ensure all frameworks, plug-ins, libraries, and software are up to date and patched, and configure the web server.

2. Default passwords are still in use on the Cisco admin portal and the Artemis web server is exposing sensitive data.

Cyber Firm Inc. Recommendations

- ➔ Prompt users to change the default Cisco password after its first use, enforce a data privacy policy, and use a web server firewall.

3. The Apache web server is vulnerable to the CVE-2019-0211 breach, the Oracle WebLogic Server is vulnerable to the CVE-2020-14882 breach, and the Microsoft Exchange Server is vulnerable to the CVE-2021-26855 breach.

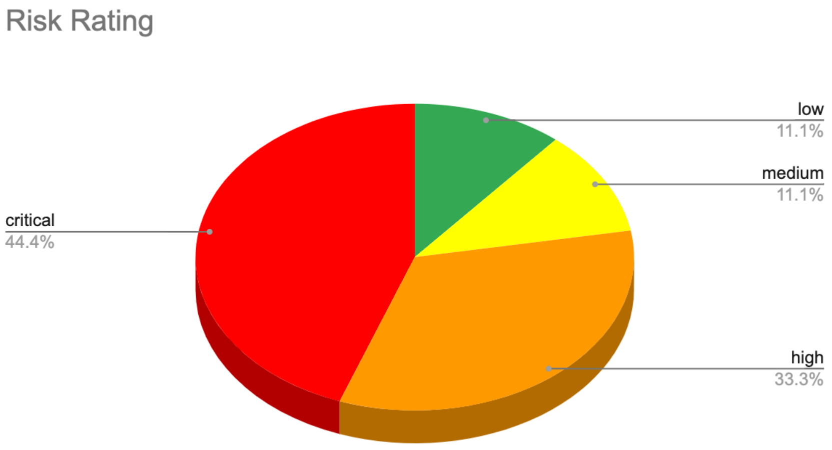
Cyber Firm Inc. Recommendations

- ➔ Update the Apache, Oracle, and Microsoft Exchange servers to a newer version.

4. There is misconfigured cloud storage (AWS security group misconfiguration, lack of access restrictions) and the Artemis web application has broken access control.

Cyber Firm Inc. Recommendations

- ➔ Limit user permissions, administer access controls, and enforce strong cloud-security policies.



Conclusion
The penetration test of ARTEMIS GAS INC. has shown that while the company is able to remediate the vulnerabilities affecting it’s network, these processes may not be 100% sufficient to mitigate risk. If exploited by an attacker, the unmitigated vulnerabilities can be used to compromise the ARTEMIS GAS INC. network.

ARTEMIS GAS INC. should further pursue opportunities to improve its vulnerability and patch management processes to ensure all critical and high risk vulnerabilities are remediated in 14 days or less.

The full list of vulnerabilities and remediation suggestions can be found in the **Artemis Project Technical Report.**

Artemis Project Technical Report

Fictional Cyber Firm Inc.

For ARTMEIS GAS INC.

V1.0

March 19th, 2023

By: Cheyenne Rohrer

Document Properties

Title	Fictional Cyber Firm Inc. Project Technical Report
Version	V1.0
Author	Cheyenne Rohrer
Pen-testers	Cheyenne Rohrer
Reviewed By	Springboard
Approved By	Springboard
Classification	Confidential

Version Control

Version	Date	Author	Description
V1.0	March 19th, 2023	Cheyenne Rohrer	Final Draft

Table of Contents

List Of Illustrations

List of Tables:

List of Figures:

1. Scope of work

This technical report details the external penetration test of Artemis's network hardware. The vulnerability assessment was conducted from a vendor host on the internet. The company's operation control center is located in Houston, Texas and monitors over 49,000 data points. All of the company's applications and servers are in the Amazon Web Services cloud or on-premises.

2. Project Objectives

The purpose of this assessment was to perform a penetration test/structured walkthrough of Artemis Gas, INC.'s technical setup and work products to find errors and improve the quality of their product and deliverable service. Vulnerabilities are given specific risk ratings based on their impact, threat, and specifications.

3. Assumptions

We will assume that the older network hardware may have unpatched vulnerabilities while the newer hardware may have configuration issues. We will also assume that Artemis may not always follow company policy regarding storage of cloud data, launching websites, and performing file transfers. The network may also be exposed to unknown risks.

4. Timeline

Penetration Testing	Start Date/Time	End Date/Time
Test 1	03/11/2023	03/18/2023

5. Summary of Findings

Value	**Number of Risks**
Low	1
Medium	1
High	3
Critical	4

Table 1 Total Risk Rating

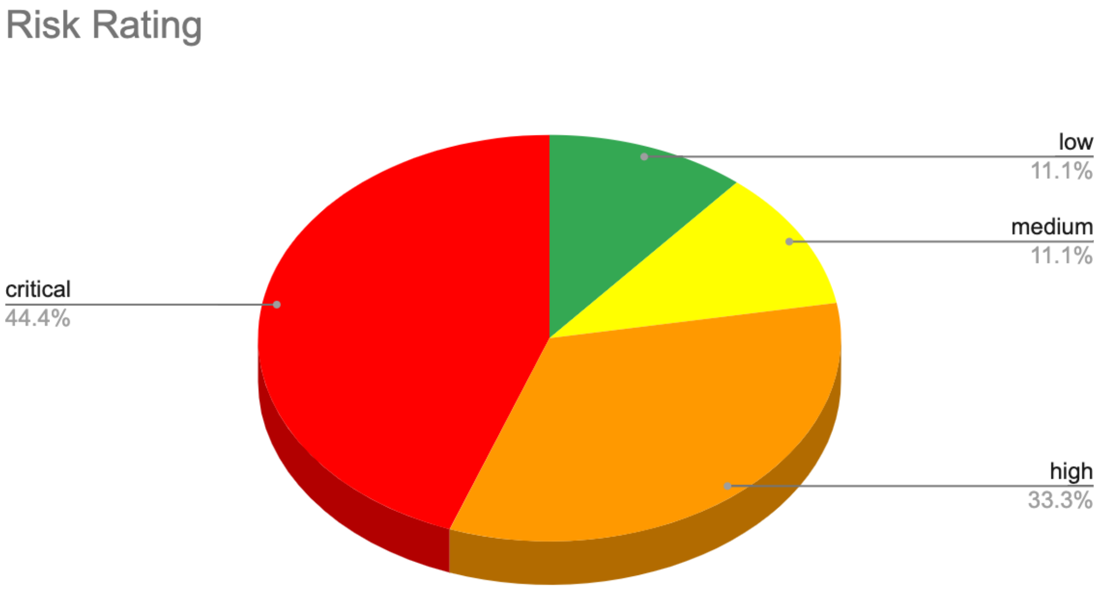


Figure 1 Total Risks

ARTEMIS GAS INC. needs to be more attentive to their network security. Multiple vulnerabilities and system weaknesses were discovered by our testing procedures. Artemis should implement multi-layer security procedures in order to protect their company's reputation and data. Below details the key findings of the external penetration test:

- ➔ ARTEMIS GAS INC. lacks multi-layer security strategies and procedures.
- ➔ There is unpatched RDP exposure to the internet. This could cause a variety of problems including: misconfigured DDoS port exposures, open port access, inferior credential hygiene, malware deploying, man-in-the-middle & ransomware attacks, unathorized collection of customer and company data, and leakages of hardware information.
    - ◆ Risk Rating: High
- ➔ The web application is vulnerable to SQL injections. Any platform that interacts with an SQL database is at risk of this. Attackers can take on fake identities, alter existing data, change pricing info, change authorization settings, delete data, etc. Login credentials as well as hardware and OS information can be leaked. Sensitive data can be compromised and ARTEMIS GAS INC.'s reputation is at risk.
    - ◆ Risk Rating: Critical
- ➔ Default passwords are still in use on the Cisco admin portal. This leaves login credentials and sensitive customer and company data vulnerable to attackers. The portal is at risk of credential stuffing and brute force attacks.
    - ◆ Risk Rating: High
- ➔ The Apache web server is vulnerable to the CVE-2019-0211 breach. Apache HTTP versions 2.4.17 to 2.4.38 are affected. Attackers can perform lateral movement and privilege escalation attacks on the system. They can also gain root access to the server by simply running scripts. They may execute unpriveleged scripts to perform a variety of malicious actions including gaining access to shared files.
    - ◆ Risk Rating: Medium
- ➔ The web server is exposing sensitive data. This issue should be delt with as soon as possible. Artemis's system is at risk of infectious malware attacks, security breaches and password leaks. Cybercriminals may also gain illegal authorized access of sensitive customer and company data. There is risk of identity fraud and DDoD attacks.
    - ◆ Risk Rating: Critical

- The web application has broken access control. This may cause several problems including: unathorized viewing of sensitive content, alterations and deletion of data, forging of cookies, and compromised login credentials. Entire system take overs are also possible.
  - Risk Rating: Low
- The Oracle WebLogic Server is vulnerable to the CVE-2020-14882 breach. Oracle Web Logic Server versions 10.3.6.0.0 to 14.1.1.0.0 are affected. Hackers have the ability to fully compromise a server. Exploitation of sensitive information is possible.
  - Risk Rating: Critical
- There is misconfigured cloud storage (AWS security group misconfiguration, lack of access restrictions). In this case, there is an increased risk of data breaches and exposure of data to the public internet. Attackers can also access and steal cloud-based data.
  - Risk Rating: High
- The Microsoft Exchange Server is vulnerable to the CVE-2021-26855 breach. The Microsoft Exchange Servers 2013, 2016, and 2019 are affected. The risks include: SSRF vulnerabilities, authentication of user access through unathauthorized HTTPS connections, unathorized permission alterations, and exposure of sensitive data.
  - Risk Rating: Critical

6. Recommendations

Fictional Cyber Firm Inc. suggests the following remediation procedures for the above findings:

- Restrict suspicious and untrusted connections of the Microsoft Exchange Server and update the software.
- Perform frequent tests of Artemis's system to ensure the system hasn't been compromised.
- Ensure sensitive data and SQL code is encrypted.

- Artemis must limit permissions where it is not necessary. This will help increase end user and company security. Monitoring of permissions is also highly recommended.
- Enforce popper logging procedures and strong cloud security policies.
- Artemis should invest in security and vulnerability alerting/testing tools. This will increase the security of their network tremendously.
- Ensure admin portals are not accessible through the internet and block admin portal access until the CVE-2020-14882 is patched. You can also update your current Oracle Web Logic Server software to a newer version.
- Be aware of suspicious HTTP requests in the network traffic. Vulnerability testing tools will alert to any suspicious HTTP requests that may appear from the CVE-202-14882 breach.
- Enforce a data privacy policy and use a web server firewall.
- Ensure all software is up-to-date and patched.
- Closely monitor server logs and frequently perform penetration testing on the webserver to check for vulnerabilities.
- In regards to the Apache CVE-2019-0211 vulnerability, we suggest updating the current Apache version to 2.4.39 or newer.
- Follow secure password practices, enforce multi-factor authentication, and routinely update and change passwords. This will increase ARTEMIS GAS INC.'s password security. It will also reduce the risk of successful credential stuffing and brute force attacks.
- Prompt users to change the default Cisco password after its first use. Never permit Default Cisco passwords to be used multiple times.
- Enforce conditional access policies.
- Prevent the use of shared database accounts with other websites and applications.
- Follow the principle of least privilege and use parameterized database queries and procedures.
- Reject requests from port 3389 and use secure tunneling software. This will reduce the risk of RDP exploitation. In addition to this, Restrict RDP user

access and priveleges and use a VPN to ensure remote users are accessing the corporate network safely. We also highly suggest enabling MFA and SSO and the use of an RDP gateway server.

7. Reconnaissance Methods:

This section outlines the techniques used to gather information about the client from an ethical penetration testing perspective. Recconaisance is completed before the vulnerability testing phase. The following OSINT resources were used to perform ethical reconnaissance for ARTEMIS GAS INC.

➔ The use of social media such as Facebook, Twitter, Reddit, Instagram, Snapchat, etc. was used to gather intelligence about ARTEMIS GAS INC.. The search option was highly utilized. Our goal was to find photos, analytics, locations, deleted posts, and any other information that would help us with the reconnaissance phase.

➔ Search engines such as Google, General People Search, and Registries were used to gather ARTEMIS GAS INC.'s username and password info, private keys, third-party configuration files, network diagrams, etc. The method of searching indexes and cache content was used to find the above information.

➔ Searching through job boards such as Linkedin, Indeed, and Glassdoor was intended to determine ARTEMIS GAS INC.'s use of cloud-based and legacy systems. The job boards helped determine the detail of their reporting structure, their use of modern applications, and the type of product and services Artemis offers. Job role descriptions were highly utilized.

➔ Company research was performed with Google, the ARTMEIS GAS INC. website, corporate communications, etc. Performing company research on ARTEMIS GAS INC. provided us with information such as their relationships with partner companies, the use of third-party-mailing services, and their marketing techniques.

- ➔ Domain and IP research was conducted with analytics, cloud resources, subdomains, geolocation services, IPv4 and IPv6, neighbor domains, etc. We were able to find information regarding ARTEMIS GAS INC.'s IT infrastructure, devices, and database and domain info.

- ➔ Several Pastebin tools were utilized to find credentials, payment information, PoC exploit code, etc. However, little information was found about ARTMEIS GAS INC. with this reconnaissance method.

8. References

Appendix A - Phase 4: Threat Assessment

file:///Users/cheyennerohrer/Downloads/Phase%204.pdf