ARTEMIS GAS, INC.

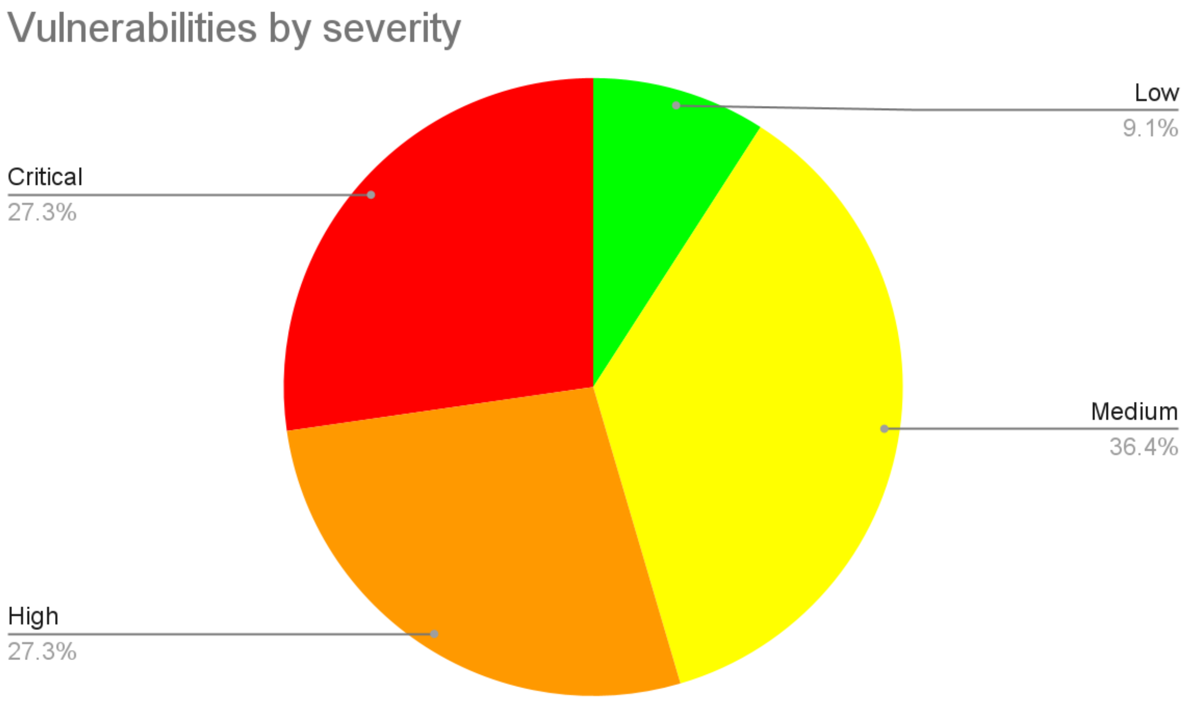
Penetration Test Technical Report

Prepared by: Jack Majure Barkley

TABLE OF CONTENTS

EXECUTIVE SUMMARY

Artemis Gas engaged Jack Barkley to provide a vulnerability assessment to determine the risk of compromise from external threats. The assessment was conducted in July of 2022. This report provides a summary of the overall findings as well as detailed recommendations on remediation.



The assessment results indicate that Artemis Gas has gaps in its patch management process, which leaves the organization vulnerable to attacks from external sources. Key findings include:

1. Unpatched RDP exposed to the internet
    a. RDP allows employees to connect to company assets from anywhere in the world. Unpatched RDP allows anyone to connect to company assets from anywhere in the world.

2. Oracle WebLogic Server vulnerable to CVE-2020-14882
    a. This vulnerability gives an attacker total control over WebLogic servers, allowing them to see everything that goes into and out of the website.
3. Microsoft Exchange Server vulnerable to CVE-2021-26855
    a. This vulnerability allows an attacker to monitor all company email traffic

These most critical findings are all remediated by software updates. Therefore, the key recommendation of this report is to develop and implement a strong patch management process. Patches rolled out as quickly as possible minimize the company's risk exposure. Additional recommendations can be found in the "Recommendations" section.

SCOPE OF WORK

This penetration test and vulnerability assessment takes the entire IT landscape of Artemis gas into account. All devices, from pipeline SCADA devices to cloud hosted web applications are in scope. The company did not request any physical or social engineering tests, so those are out of scope. Testing was conducted using industry standard best practices and technologies including Nmap, Nessus, OpenVAS, swaks, enum4linux, and fierce.

PROJECT OBJECTIVES

The company’s growth has negatively impacted their security posture. The objective of this test was to find any current vulnerabilities and suggest remediation activities. Since the company operates internationally, compliance with GDPR was also a concern. This report ranks and quantifies the risk associated with each vulnerability, so that informed decisions can be made about risk mitigation, transference, or acceptance.

ASSUMPTIONS

Artemis Gas is a large company with international recognition. Therefore, we can assume that threat actors will use highly sophisticated tools and methods to attempt exploits. The company also handles a large amount of intellectual property and PII, so we assume that these types of data are a high priority to secure.

TIMELINE

The testing period was one week long. Day one involved reconnaissance on the network, enumerating hosts and mapping the network landscape. On day two, targets were identified and scans were run against those targets. Day three reviewed these scan results and identified vulnerabilities. Day four consisted of listing discovered vulnerabilities and rating their risks, along with suggested remediation actions. Day five was spent writing this report.

SUMMARY OF FINDINGS

Overall, nine vulnerabilities were discovered on the network. Of those nine, four can be remediated with a software update. Three findings have a CVSS score of nine or above, so these should be prioritized for remediation activity.

DETAIL FINDINGS

1. Unpatched RDP is exposed to the internet
    a. CVSS Score: 9.1 (High)
    b. Detail: RDP access grants attackers remote access to sensitive files, and can be used as a pivot point for higher privileged access.
2. Web application is vulnerable to SQL Injection
    a. CVSS Score: 8.1 (High)
    b. Detail: Reverse shells with SQL are trivial, and command line access to a database to a database means easy exfiltration
3. Default password on Cisco admin portal
    a. CVSS Score: 5.3 (Medium)
    b. On its own, the firewall won't have much access or visibility into the network. However, if the firewall is disabled or modified to allow malicious activity through, the risk is much greater
4. Apache web server vulnerable to CVE-2019-0211
    a. CVSS Score: 7.8 (High)
    b. This exploit grants the ability to execute arbitrary code as root.
5. Web server is exposing sensitive data

    a. CVSS Score: 7.5 (High)
    b. Exposed sensitive data is out of compliance with GDPR.

6. Web application has broken access control
    a. CVSS Score: 6.5 (Medium)
    b. Attacker would first need login credentials to exploit broken access control.
7. Oracle WebLogic Server vulnerable to CVE-2020-14882
    a. CVSS Score: 9.8 **(CRITICAL)**
    b. Successful exploit results in takeover of WebLogic server. All I/O could then be monitored and compromised.
8. Misconfigured cloud storage (AWS security group misconfiguration, lack of access restriction)
    a. CVSS Score: 4.6 (Low)
    b. Greatest threat here would be from an insider. Still worth looking at, but priority is low.
9. Microsoft Exchange Server vulnerable to CVE-2021-26855
    a. CVSS Score: 9.8 **(CRITICAL)**
    b. Compromised exchange server would expose all internal communications. Intellectual property theft is very likely.

RECOMMENDATIONS

1. Unpatched RDP is exposed to the internet
    a. Patch all RDP clients to the latest version.
    b. Create and maintain an access control list for employees who need to use RDP.
2. Web application is vulnerable to SQL Injection
    a. Implement input sanitization on all SQL function calls
    b. Monitor network using Snort to flag on SQL attacks
3. Default password on Cisco admin portal
    a. Change the password.
    b. Company is phasing out Cisco devices. Ensure new Fortigate devices also have default passwords changed.
4. Apache web server vulnerable to CVE-2019-0211
    a. Patch web server to the latest available version of Apache.
    b. Create patch management process to automate patch deployment
5. Web server is exposing sensitive data
    a. Evaluate what data is already exposed and notify affected parties, as required by law
    b. Ensure all communication is encrypted with a strong cipher suite
6. Web application has broken access control
    a. Audit user profiles for current privileges. Watch out for privilege creep, and remove any unnecessary permissions
    b. Audit user roles and ensure they match current company data protection

standards

c. Fix web application so only those who need access have access

7. Oracle WebLogic Server vulnerable to CVE-2020-14882
    a. Rollout October 2020 critical patch update from Oracle
    b. Create patch management process to automate patch deployment
8. Misconfigured cloud storage (AWS security group misconfiguration, lack of access restrictions)
    a. Review cloud user profiles for privilege creep, remove excess permissions
    b. Create access restrictions based on who needs access to data, use principle of least privilege
9. Microsoft Exchange Server vulnerable to CVE-2021-26855
    a. Patch on-prem exchange server to latest version
    b. Current Exchange environment is hybrid cloud, consider moving entirely to cloud so updates are no longer an issue