CONFIDENTIAL

Artemis Gas Inc.

Penetration Test Conducted by Pappas Security

EXECUTIVE SUMMARY

Artemis Gas Inc. engaged Pappas Security to provide a vulnerability assessment to determine the risk of compromise due to internal (insider) or external threats. The assessment was conducted in September 2021. Pappas Security performed an external network vulnerability assessment from the security analyst's host from the internet and an internal network vulnerability assessment from the security analyst's laptop wired to Artemis's internal corporate network. This report provides a summary of the overall findings and displays statistical charts for all detected vulnerabilities. Recommendations will be addressed for the critical and high-risk vulnerabilities.

The assessment results indicate that Artemis Gas Inc. will be vulnerable to attacks from both external and internal threat actors unless it addresses the following:

- Improve patch management procedures for critical updates to the operating system and services
- Put proper security controls in place for new network devices
- Implement security controls during the software development life to address code injection vulnerabilities
- Configure IAM permissions to remediate insecure cloud services

Pappas security identified 3 critical and 2 high risk vulnerabilities on the external network and 1 high risk vulnerability on the internal network. **Pappas security recommends remediation of the critical and high risk vulnerabilities within the next 30 days to reduce the risk of exposing the networks to attacks.**

Key Summary Findings and Recommendations:

1. Unpatched Windows public-facing web server and exchange server were found. Leaving these hosts and services unpatched leaves the internal network vulnerable to attacks that would result in a data breach or compromise the entire internal IT infrastructure.

   VENDOR RECOMMENDATIONS

   Artemis must confirm that the appropriate Windows operating system and Exchange Server patches are installed. Management will need to put a patch management program in place.

2. The SQL statements and PHP scripts are vulnerable to malicious attacks. Input validation and dynamic code testing has to be performed throughout the software development life cycle.

   VENDOR RECOMMENDATIONS

   Management needs to incorporate secure code at the very beginning of the software development process by using an agile framework.

3. Weak configurations on Cisco router and overly-permissive IAM policies on AWS.

   VENDOR RECOMMENDATIONS

   Management needs to inventory all new assets (servers, wired and wireless network devices,IoT) in the company and address any weak default configurations. Management needs to apply least privilege to the IAM permissions on AWS.

Conclusion

The assessment has shown that while Artemis Gas Inc. has the ability to remediate vulnerabilities affecting it's infrastructure, these procedures may **NOT** be all-inclusive and adequately effective to mitigate risk. These unmitigated vulnerabilities, if exploited by an attacker, can be used to undoubtedly compromise the entire **ARTEMIS** network.

Artemis Gas Inc. will need to go beyond the required security remediation steps. It needs to be proactive in dealing with security vulnerabilities by consistently training it's staff, working with outside security vendors, and consistently performing research on the latest security threats. More detailed remediation steps are outlined in Vulnerabilites_Capstone_Phase_4.xlsx. Pappas Security has included a pie chart and bar chart illustrating how the critical and high risk vulnerabilities are outnumbering the medium risk vulnerabilities.

Pie chart shows the 9 vulnerabilities found at Artemis Gas Inc. and their severity level.

Vulnerability Pie Chart