Phase 5.2

Executive Summary

EXECUTIVE SUMMARY

Artemis INC requested to provide a vulnerability assessment to discover all the potential risks of compromise loss due to internal and external threats. This vulnerability assessment took place in January of 2023. An external network vulnerability assessment will be performed on the internet, and an internal network vulnerability assessment will be performed with a laptop connected to Artemis's internal corporate network. This report summarizes the overall findings of the vulnerabilities discovered by the scanning tools, as well as detailed findings and recommendations for high-risk vulnerabilities will be noted.

The assessment results indicate that Artemis INC may be vulnerable because of its patch and vulnerability management processes. These vulnerabilities could cause and lead to attacks from both internal and external sources. The assessment identified six **critical**-risk and one **high**-risk vulnerability. Remediation of critical and high-risk vulnerabilities within the next month is recommended to reduce the risk of exposing the network to attacks.

Key Summary Findings and Recommendations:

1. Data centers such as Cairo and Singapore use older network hardware. It uses Remote Desktop Protocol (RDP) instead of Zscaler, like other data centers in Houston and Paris. The RDP is unpatched and exposed to the internet, leaving potential vulnerabilities such as information disclosure to full system compromise.

   RECOMMENDATIONS
   Artemis should change all data centers to use Zscaler, disable all RDP, and close down port 3389 with a firewall. Use an antivirus system that features Remote Access Shield. Continue to Section E: Detailed Reported for further technical details.

2. The company's main website (Artemis.com) login page is vulnerable to SQL injection attacks because the business unit does not follow company policy when creating the website. This vulnerability can lead to information disclosure. The attacker can gain access to the whole SQL database.

   RECOMMENDATIONS
   Artemis should use techniques such as prepared statements with parameterized queries, allowlist input validation, properly stored procedures, and escape all user input to prevent SQLi. Continue to Section E: Detailed Reported for further technical details.

3. Newer network equipment is not configured properly, such as Fortinet using default credentials to log in to their admin portal. This vulnerability can result in unwanted access that leads to full system compromise.

   RECOMMENDATIONS
   Artemis should change the default credentials into a unique password for their Fortinet equipment. Continue to Section F: Detailed Reported for further technical details.

4. Sensitive data are exposed on the Artemis Web server by lazy admins who like to do their own things, resulting in a lack of encryption. This vulnerability can lead to all data being compromised and exposed to SQLi attacks, broken access control attacks, ransomware attacks, phishing attacks, insider threat attacks, etc. Continue to Section G: Detailed Reported for further technical details.

   RECOMMENDATIONS
   Artemis should encrypt all sensitive data at rest and use strong ciphers on the web server page. Disabling caching for the response that store sensitive data can also mitigate this vulnerability. Continue to Section F: Detailed Reported for further technical details.

5. Artemis's primary ERP system runs on Oracle 12c. The Oracle WebLogic Server is version 12.2.1.4.0, which is vulnerable to CVE-2020-14882. This vulnerability bypasses the authentication and compromises the whole Oracle WebLogic Server.

   RECOMMENDATIONS
   Artemis should install the critical patch update that was released in October 2020. Continue to Section F: Detailed Reported for further technical details.

6. The vendor found misconfigured security group policy on the AWS cloud storage. Allowing ports 22 and 3389 to be open. This vulnerability can cause cloud-based data to be beached.

   RECOMMENDATIONS
   Artemis should only allow specific IP address access to the secure shell and RDP ports. Section F: Detailed Reported for further technical details.

7. Artemis uses a Microsoft Exchange server on-prem for messaging. The Vendor found Artemis is using the unpatched version of the Microsoft Exchange server version 2019. The unpatched version is vulnerable to CVE-2021-26855. This vulnerability can bypass the authentication allowing hackers to download user email and gain full access to the mail server.

   RECOMMENDATIONS
   Artemis should install the mandatory patches for the affected version. Section F: Detailed Reported for further technical details.

Conclusion

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 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. A full list of vulnerabilities and detail can be found in the detailed report.