Securely Transmitting Data: Executive Summaryfor Artemis’s Senior Management.

Vincent Kiweesi

Capstone

May 26, 2023

Vincent Kiweesi

Cybersecurity Analyst

Umass Global

May 23rd, 2023

Executive Summary

Artemis's Senior Management

This executive summary provides a high-level overview of the company vulnerability assessment to determine the risk of compromise due to internal or external threats conducted in May of 2023 threats and key findings regarding the cybersecurity posture of Artemis. The purpose is to deliver a concise and clear understanding of the risks and potential impact to enable informed decision-making by senior management. The assessment results indicate that Artemis may have process gaps in its patch and vulnerability management processes, which could leave the organization vulnerable to attacks from both internal and external sources. 3 ​critical​ and 5 ​high​-risk vulnerabilities were identified on the internal network and 1 Moderate-risk vulnerabilities on the external networks. ​Remediation is recommended of the critical- and high-risk vulnerabilities within the next 30 days to reduce the risk of exposing the network to attacks.

**Key Findings**

Based on the comprehensive assessment conducted on Artemis, the following key findings have been identified:

**Vulnerability Assessment:**

* Overall, Artemis has a high vulnerability posture, with a few critical vulnerabilities identified.
* 33% of the vulnerabilities discovered are classified as high severity.
* The top three vulnerable areas are outdated software, weak access controls, and unpatched systems.

**Threat Analysis:**

* The threat landscape targeting organizations like Artemis is highly dynamic and evolving.
* Malware infections, social engineering attacks, and unauthorized access attempts are prevalent threats.
* Advanced persistent threats (APTs) pose a significant risk, targeting valuable intellectual property and customer data.

**Current Threat Environment:**

* Artemis operates in an industry that is frequently targeted by cybercriminals due to the value of the data it handles.
* The organization is at risk of data breaches, financial losses, reputational damage, and regulatory non-compliance.
* External threats, such as nation-state actors and organized cybercrime groups, pose an ongoing risk.

**Risk Assessment**

 The risk assessment conducted on Artemis reveals the following risk profile:

**Overall Risk Level:** Moderate

* Artemis has implemented several security controls, reducing the overall risk level to a moderate range.
* However, critical vulnerabilities and evolving threats indicate a need for continuous monitoring and improvement.

**Identified Risk Areas:**

* Outdated software poses a significant risk, as it can be exploited by adversaries to gain unauthorized access.
* Weak access controls increase the likelihood of unauthorized activities and potential data breaches.
* Unpatched systems create vulnerabilities that can be exploited by threat actors to compromise Artemis' infrastructure.

**Recommendations**

  To mitigate the identified risks and enhance the cybersecurity posture of Artemis, the following recommendations are proposed:

**Vulnerability Management:**

* Implement a robust patch management program to ensure timely updates and address known vulnerabilities.
* Conduct regular vulnerability assessments and penetration testing to proactively identify and remediate weaknesses.

**Access Control:**

* Strengthen access controls through the implementation of multi-factor authentication (MFA) and least privilege principles.
* Regularly review and update user access privileges to minimize the risk of unauthorized access.

**Security Awareness Training:**

* Provide comprehensive security awareness training to all employees to mitigate the risk of social engineering attacks.
* Foster a culture of cybersecurity awareness and promote reporting of suspicious activities or incidents.

**Conclusion**

Artemis faces multiple high-risk vulnerabilities across its network infrastructure and web applications. It is important to address these vulnerabilities promptly to mitigate the risk of unauthorized access, data breaches, and potential system compromise. We strongly recommend applying the recommended patches, implementing proper access controls, also ensuring that all critical- and high-risk vulnerabilities are remediated within 30 days or less, and regularly reviewing and updating security configurations.

For a detailed analysis and technical information, please refer to the attached Detailed Technical Report. If you have any questions or require further clarification, please do not hesitate to contact Vincent Kiweesi at vkiweesi@gmail.com.

Sincerely,

Vincent Kiweesi

Cybersecurity Analyst