# Executive Summary

Arthemis engaged Rashawn to provide a vulnerability assessment (“Assessment”) to determine the risk of compromise due to internal or external threats. The assessment was conducted in January of 2020. Rashawn performed an external network-layer vulnerability assessment from a Rashawn host on the internet and an internal network-layer vulnerability assessment from an Rashawn laptop connected inside Arthemis internal corporate network. This report provides a summary of the overall findings and statistics for all identified vulnerabilities, as well as the detailed findings and recommendations for critical and high-risk vulnerabilities.

The assessment results indicate that Arthemis 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. Rashawn identified 7 critical- and 6 high-risk vulnerabilities on the internal network and 12 Moderate-risk vulnerabilities on the external networks. Rashawn recommends remediation of the critical- and high-risk vulnerabilities within the next 30 days to reduce the risk of exposing the network to attacks.

## Vendor Recommendations

Patch these vulnerabilities in accordance with their risk level and reevaluate current patch management tools and practices. Arthemis should implement a comprehensive patch management tool and program if one does not already exist. Management should provide oversight to confirm the vulnerability and patch management programs continue to be maintained.

1. Unpatched RDP is exposed to the internet
2. Web application is vulnerable to SQL Injection
3. Default password on Cisco admin portal
4. Apache web server vulnerable to CVE-2019-0211
5. Web server is exposing sensitive data
6. Web application has broken access control
7. Oracle WebLogic Server vulnerable to CVE-2020-14882
8. Misconfigured cloud storage (AWS security group misconfiguration, lack of access restrictions)
9. Microsoft Exchange Server vulnerable to CVE-2021-26855

## Conclusion

The Assessment has shown that while Arthemis has the ability to patch and remediate vulnerabilities affecting its environment, these processes may not be comprehensive or sufficiently effective to mitigate risk. These unmitigated vulnerabilities, if exploited by an attacker, can be used to potentially compromise the full Arthemis network.