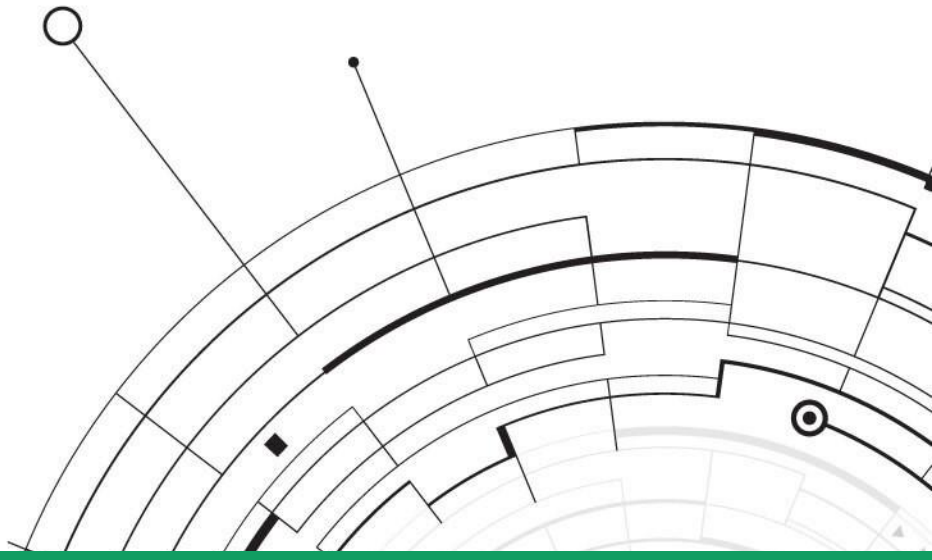
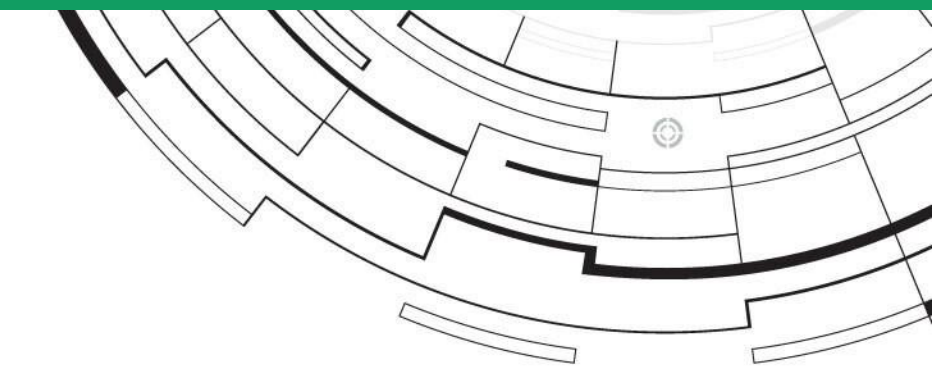


Internal Pentest + Vulnerability Assessment

EXECUTIVE SUMMARY



Company

Feb 27, 2024

Copyright

Confidentiality

This document contains confidential company information of a proprietary and sensitive nature. As such, this document should be afforded the security and handling precautions that a confidential document warrants. This document should have a controlled distribution to relevant parties only and should not be copied without written permission. RSI treats the contents of a security audit as confidential company material and will not disclose the contents of this document to anyone without written permission.

Assessment Project Team

Below is a list of contacts that were involved in this engagement. Should you have any questions pertaining to the content of this document or any project and non-project-related items, please feel free to reach out to the necessary project contacts.

Primary Point of Contact	
Name:	David Burgeson
Title:	CEO
Office:	(254) 222-2222
Email:	gojenne@rsitex.com
Primary Point of Contact	
Name:	Angela Hogaboom
Title:	Chief Security Officer
Office:	(512) 333-3333
Email:	gojenne@rsitex.com

Executive Summary

Company has requested the assistance of Renaissance Systems Inc. to perform a comprehensive security assessment to assist with evaluating the cyber risks presented within the tested environment(s). The objective of this engagement was to determine if any identified threats could be used to mount an attack against the organization that could lead to the disclosure of sensitive information or access to critical information systems.

Included in this Executive Summary report is a high-level overview of the results that were observed during this assessment. A copy of more specific information pertaining to technical findings and remediation details are documented within the Technical Report as well as the Vulnerability Tracking Report.

Engagement Scope of Work

Prior to beginning the assessment, Renaissance Systems Inc. and Company agreed to a scope of work to define the specific assessment phases. The table below outlines the engagement scope of work and details entailed within each assessment phase that was conducted as part of this engagement.

Assessment Component	Assessment Phases
Internal Network Security Assessment	During this phase, security weaknesses within the internal network environment are identified to attempt discovering sensitive and/or valuable information within the environment. This phase includes man-in-the-middle attacks, as well as exploitation of patching, authentication, as well as configuration deficiencies. Additionally, a penetration test and vulnerability assessment is conducted to identify and exploit security weaknesses. D **Internal Network Penetration Test** - A penetration test was conducted to identify the potential impact of exploiting any identified vulnerabilities. Only exploits that are deemed safe were executed during this phase. D **Vulnerability Assessment** - A vulnerability assessment was also performed against the list of systems provided for the scope for testing. This vulnerability assessment attempted to identify, but not exploit, security vulnerabilities that exist within the environment.

Engagement Statistics

The information below displays overall statistics that were recorded as part of this engagement. Following the statistics, Renaissance Systems Inc. has summarized all of the threats identified.

Internal Network Security Assessment

The information below provides a high-level overview of the assessment results recorded as part of this engagement. Following this section is a summary of all the threats identified and their potential risk to your organization.

Overall Severity Ranking

ASSESSMENT SCHEDULE

Tue, January 07, 2025
07:10 AM CT

Immediate remediation or mitigation is required. Exploitation of identified vulnerabilities require minimal effort from an attacker and pose a significant threat. A successful attack could result in unauthorized access to systems and/or valuable data.

Engagement Results Charts

To help Company understand the severity of the threats identified during testing, Renaissance Systems Inc. has included an over-all summary chart below that displays a comparison of the report findings as well as the vulnerabilities that were discovered.

Internal Network Security Assessment Results

PenTest Findings

The following chart displays the overall severity of the report findings that were documented as part of the penetration testing efforts.

C	3	CRITICAL	H	0	HIGH
M	1	MEDIUM	L	0	LOW
I	1	INFO			

As part of the penetration test, Renaissance Systems Inc. also performed a vulnerability assessment to provide additional value and insight as to the vulnerabilities that were identified by our vulnerability scanner. This vulnerability scan included the discovery of common security vulnerabilities that are publicly documented with Common Vulnerabilities and Exposures (CVE) scores.

VULNERABILITY ASSESSMENT FINDINGS

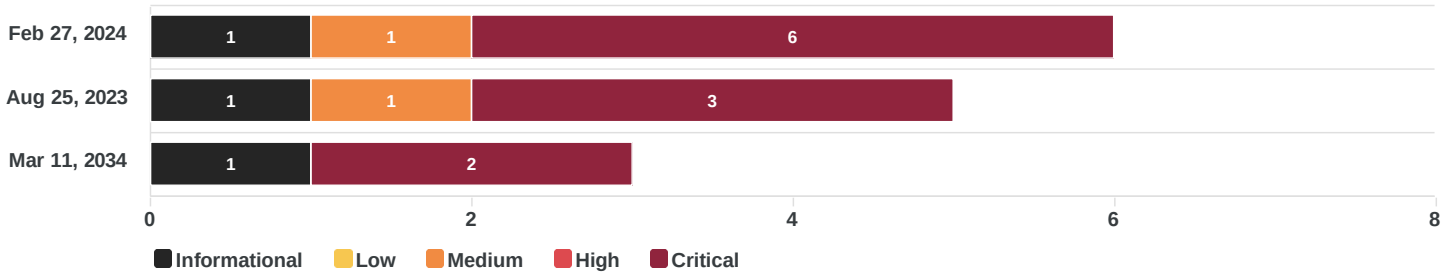
31 TOTAL

0 CRITICAL	0 HIGH	4 MEDIUM	2 LOW	25 INFO

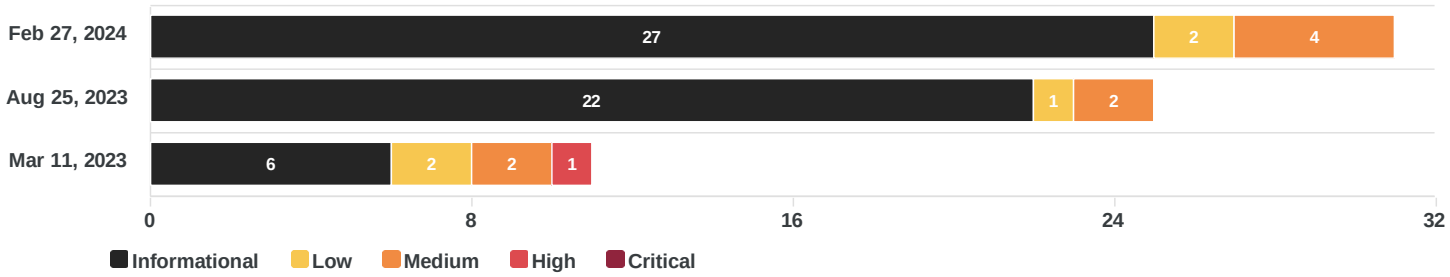
Comparison Charts

To help Company understand the trend of the PenTest Findings and vulnerabilities discovered in the past as part of this on-going engagement, Renaissance Systems Inc. has provided trend data in this section of the report.

History of PenTest Findings



History of Vulnerability Assessment Findings



Engagement Results Summary

To summarize the results, Renaissance Systems Inc. has grouped all of the findings from the penetration test into rollup findings. These rollup findings can be used to quickly determine the root cause of the issues identified in the technical report. By implementing a remediation strategy for the findings based on the rollup issues identified below, Company's security posture would be greatly reduced.

Internal Network Security Assessment

Category	Summary
Configuration Deficiencies	Configuration weaknesses were identified that could potentially lead to a successful compromise of systems and/or data within the tested environment. Although some of the configuration weaknesses may be exploitable in limited circumstances, the potential impact of a successful attack could be relatively high.
Egress Filtering Deficiencies	Testing identified that excessive services are accessible on the public Internet from the internal network environment. This could allow for an attacker to circumvent security controls by using alternative communication channels. Furthermore, a compromised system may be able to use such alternative communication channels to exfiltrate sensitive information.

Remediation Roadmap

For each assessment conducted, Renaissance Systems Inc. provided a remediation roadmap to help Company understand the issues within the respective environment and the overall remediation strategies that should be implemented to resolve the issues identified during the penetration test. It should be noted that the remediation strategies below apply to multiple issues identified within the technical report and can greatly reduce the overall attack surface once successfully implemented.

Internal Network Security Assessment

Issue	Remediation Strategy
Configuration Deficiencies	Implement or improve a security configuration baseline that adheres to security best practices and industry standards such as National Institute of Standards and Technology (NIST). This security configuration baseline should ensure that no services and/or systems are deployed within the environment until a thorough configuration review has been performed.
Egress Filtering Deficiencies	Ensure that the organization's network firewalls restrict outbound access to the public Internet to services that are required for business operations. For services that are required for business operations, the organization should document these in a policy and procedure so that business justifications are communicated and understood within the organization. Any adjustments to these configurations should be documented in a change management program to establish an audit trail.