Robert A. Kalka

Metropolitan Skyport

Security Assessment Briefing

Team XX

1/14/24

OUR TEAM






Timeline

9/27/23

Contract Start

1/12/24 - 1/13/24

Follow-up Engagement

First Penetration Test

11/11/23

Summary of Engagement

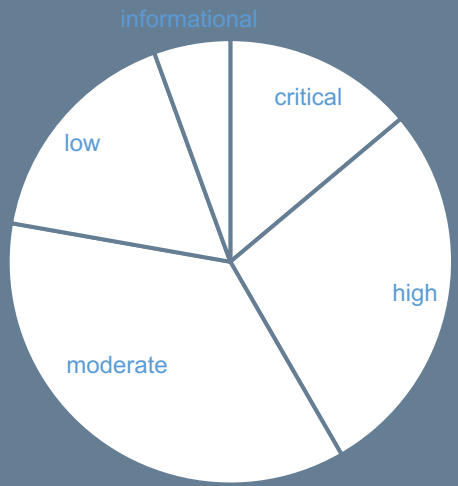
- Follow-up engagement of the RAKMS corporate, train, user, and guest networks
- Testing the strength of the network security infrastructure
- Reassessing known vulnerabilities from the previous assessment

Key Findings

- Many of the issues from the previous assessment have been addressed
- We found new and resurfaced vulnerabilities that compromise customer and company data
- Various compliance violations in applications, databases, and servers

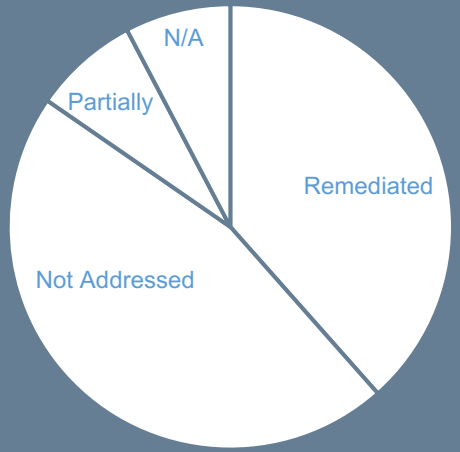
Assessment Summary

14% Critical



Finding Breakdown

38% Remediated



Remediation Breakdown

Risk Framework

- Common Vulnerability Scoring System (CVSS v3)
  - Industry standard
  - Numerical scale with broad classifications
  - Various factors accounted for

Compliance

PCI-DSS

Protecting cardholder data

SOC 2

Customer data management

TSA

Improve cybersecurity resilience

Key Strengths

Network Segmentation

Vital networks separated from guest access

Linux System Security

Up-to-date software

Monitoring Team

Rapid response to malicious activity

Recommendations

Outdated System & App Software

Vulnerable software

Mismanaged privileges

Application Logic

Web applications were vulnerable to well documented OWASP vulnerabilities

Syncing Development to Management

Many application vulnerabilities came from misunderstanding of business logic

Thank You

Questions?