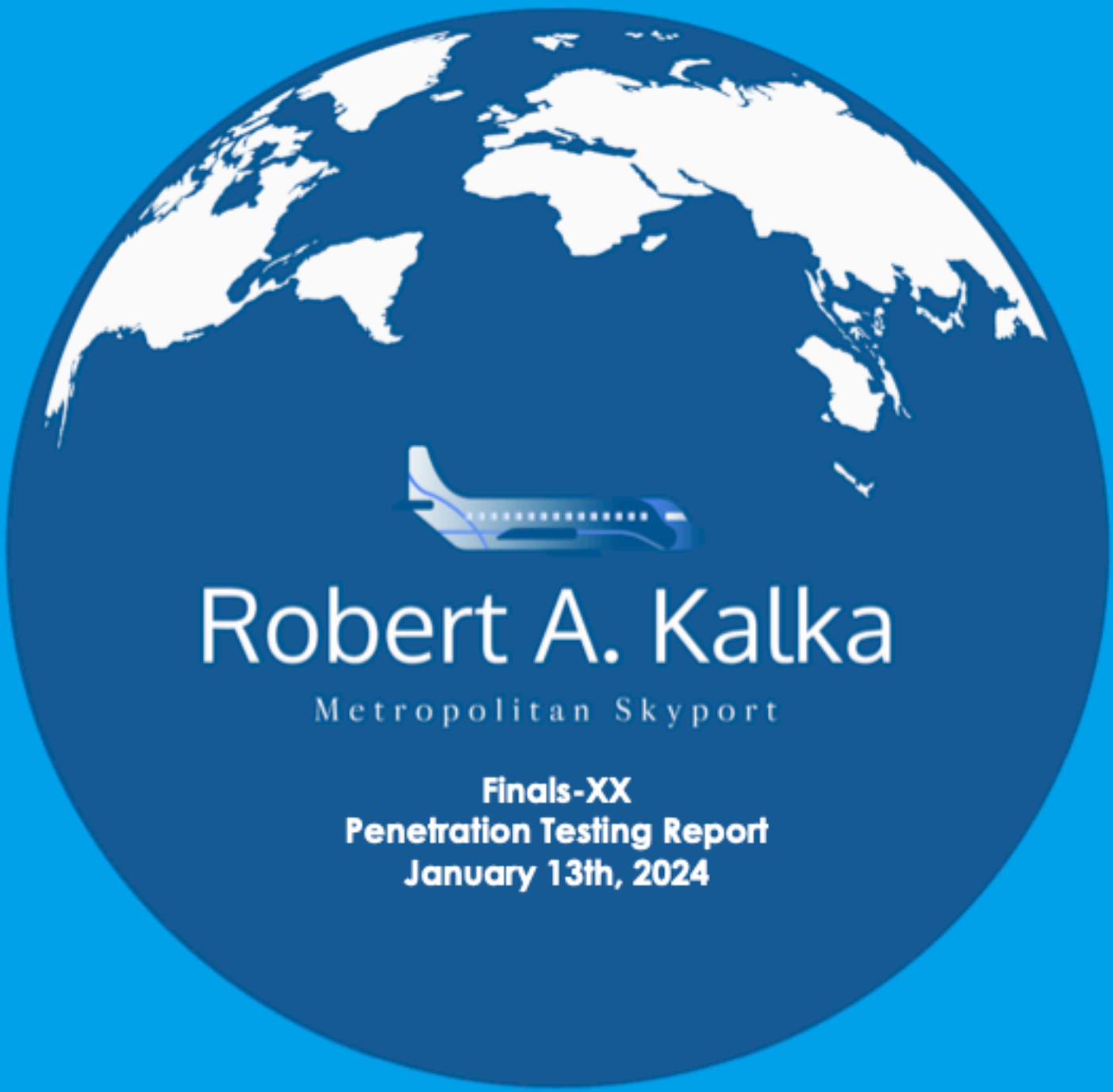


Robert A. Kalka

Metropolitan Skyport

Finals-XX
Penetration Testing Report
January 13th, 2024

Limitations on Disclosure and Use

This report contains information concerning potential vulnerabilities of Robert A Kalka Metropolitan Skyport's (RAKMS) network and systems and methods of exploiting them. Finals-XX recommends that special precautions be taken to protect the confidentiality of both this document and the information contained herein. Finals-XX has retained and secured a copy of the report for customer reference. RAKMS has received all other copies.

Security assessments are an uncertain process based on the system state at the time of the test, currently available information, and known threats. All information systems, which by their nature are dependent on human beings, are vulnerable to some degree. Therefore, while Finals-XX considers the major security vulnerabilities of the analyzed systems to have been identified, there can be no assurance that any exercise of this nature will identify all possible vulnerabilities or propose exhaustive and operationally viable recommendations to mitigate those exposures.

The analysis set forth herein is based on the technologies and known threats as of the date of this report. As technologies and risks change over time, so will the vulnerabilities associated with the operation of RAKMS' systems described in this report and the actions necessary to reduce the exposure to such vulnerabilities. Finals-XX makes no undertaking to supplement or update this report based on changed circumstances or facts of which Finals-XX becomes aware after the date hereof, absent a specific written agreement to perform a supplemental or updated analysis.

Contact Information
+1 (555) 555-5555

Table of Contents

Document Control Information

Document Details	
Company:	Robert A Kalka Metropolitan Skyport
Document Title:	Robert A Kalka Metropolitan Skyport Penetration Test Report
Version:	1.0
Date Edited:	January 13th, 2024
Authors:	Finals-XX
Classification:	Confidential

Recipients	
Name:	Ted Striker
Title:	Director of Security and Technology

Executive Summary

Robert A. Kalka Metropolitan Skyport (RAKMS) has enlisted the services of Finals-XX to conduct a second internal network penetration test on its information technology assets. Our team has observed improvements since our first assessment showing a total of **8** remediated vulnerabilities since our first assessment. There was a total of **5** different way to gain the highest privilege account within the domain

As well as the findings of security vulnerabilities, our team noted many breaches of compliance that would incur fines if not remediated. Our team found a total of **4** compliance violations resulting in an estimated fine amount of <>

Timeline:
Engagement Began 2024-1-12 9:30 AM EST

Engagement Concluded 2024-1-13 5:45 PM EST

Report Delivered 2024-1-13 11:59 PM EST

Finals-XX found and identified a total of **30** vulnerabilities within the scope of this engagement, which is broken down by severity below:

Critical	High	Medium	Low	Informational
5	10	14	1	0

Strategic Recommendations

In order to improve the security posture of RAKMS, Finals-XX recommends:

Immediate Actions:

- Patch critical findings in the Domain Controller
- Fix broken access control across the environment
- Implement a strong password policy

Long-Term Strategies:

- Regular pentests to continuously improve security posture of RAKMS
- Implementation of MFA on all accounts to make compromises 99.9% less likely (source Microsoft)
- Improve web servers by moving to HTTPS using the Domain Controllers ADCS to create secure, trusted certificates across RAKMS' Network

Compliance and Regulatory Overview

TSA Cybersecurity Requirements

The recent cybersecurity amendment issued by the Transportation Security Administration (TSA) carries significant implications for Robert A Kalka Metropolitan Skyport, as a TSA-regulated airport operator. This amendment underscores the critical need for heightened cybersecurity measures in the aviation sector, particularly in light of persistent threats against U.S. critical infrastructure. Below, we assess the extent to which the current cybersecurity posture aligns with these newly introduced regulations.

Requirement	Status	Associated Findings
Develop network segmentation policies and controls to ensure that operational technology systems can continue to safely operate in the event that an information technology system has been compromised.	❌	RAKMS-007
Create access control measures to secure and prevent unauthorized access to critical cyber systems.	❌	RAKMS-004 RAKMS-010 RAKMS-011 RAKMS-020 RAKMS-025
Implement continuous monitoring and detection policies and procedures to defend against, detect, and respond to cybersecurity threats and anomalies that affect critical cyber system operations.	✅	N/A
Reduce the risk of exploitation of unpatched systems through the application of security patches and updates for operating systems, applications, drivers and firmware on critical cyber systems in a timely manner using a risk-based methodology.	❌	RAKMS-002

Payment Card Industry Data Security Standard (PCI DSS)

PCI DSS at a Glance
The Payment Card Industry Data Security Standard (PCI DSS) is a set of standards that ensures companies process, store, and transmit cardholder data securely. Most major payment card brands enforce PCI DSS compliance, and any company handling cardholder data must comply with these standards. Finals-XX followed the PCI DSS Penetration Testing Guidance during the engagement and kept a detailed record of all violations associated with the technical findings, which can be found below. Unaddressed PCI DSS violations lead to risks, including, but not limited to, monthly fines of up to $100,000, potential lawsuits, damage to the company's reputation, and a weakened security posture.

PCI DSS Prioritized Approach
The Prioritized Approach for PCI DSS serves as a roadmap to achieve PCI DSS compliance as described by specific milestone criteria pertaining to the PCI DSS requirements. According to the criteria listed in the document and the engagement findings, Finals-XX has determined RAKMS to be in phase 1. Finals-XX suggests RAKMS use the Prioritized Approach milestones as a roadmap for its compliance strategy. The following figure shows the full list of high-level goals associated with each milestone:

Phase	Goal
1	Remove sensitive authentication data and limit data retention.
2	Protect systems and networks, and be prepared to respond to a system breach.
3	Secure payment card applications.
4	Monitor and control access to your systems.
5	Protect stored cardholder data.
6	Finalize remaining compliance efforts and ensure all controls are in place.

General Data Protection Regulation (GDPR)

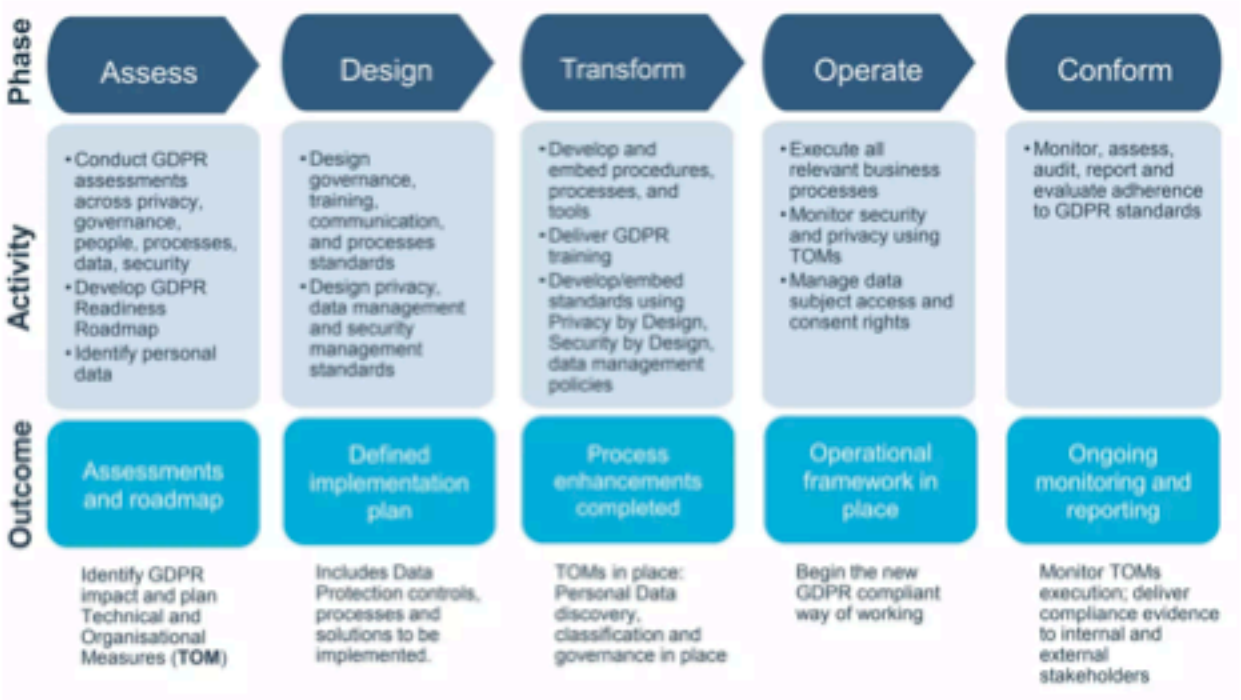
GDPR at a Glance
The General Data Protection Regulation (GDPR) is a comprehensive data protection framework that applies to the processing of personal data within the European Union (EU) and the European Economic Area (EEA). It encompasses a wide range of data

protection requirements, including the lawful and transparent processing of personal data, data subject rights, data breach notification, and privacy by design principles.

RAKMS, as an airport, handles a significant volume of personal data, which includes information related to passengers, employees, and various stakeholders. The GDPR is of paramount importance to RAKMS because it governs how personal data should be collected, processed, and protected. For a detailed breakdown of compliance violations associated with each finding, see the detailed finding breakdown below.

GDPR Readiness

IBM's GDPR framework serves as a roadmap to achieve GDPR compliance as described by specific milestone criteria pertaining to the GDPR requirements. According to the criteria of the framework and the engagement findings, Finals-XX has determined RAKMS to be in the Assess phase. Finals-XX suggests RAKMS use the framework milestones as a roadmap for its compliance strategy. The following figure shows the full list of high-level goals associated with each milestone:



Technical Overview

Scope

The scope of this penetration test was comprehensive and aimed to provide a thorough understanding of RAKMS' security posture. The scope included four IP ranges:

IP Range (CIDR)	Name
10.0.0.0/24	Corporate Network
10.0.1.0/24	User Network
10.0.20.0/24	Train Network
10.0.200.0/24	Airport Guest Network
Amazon Web Services	

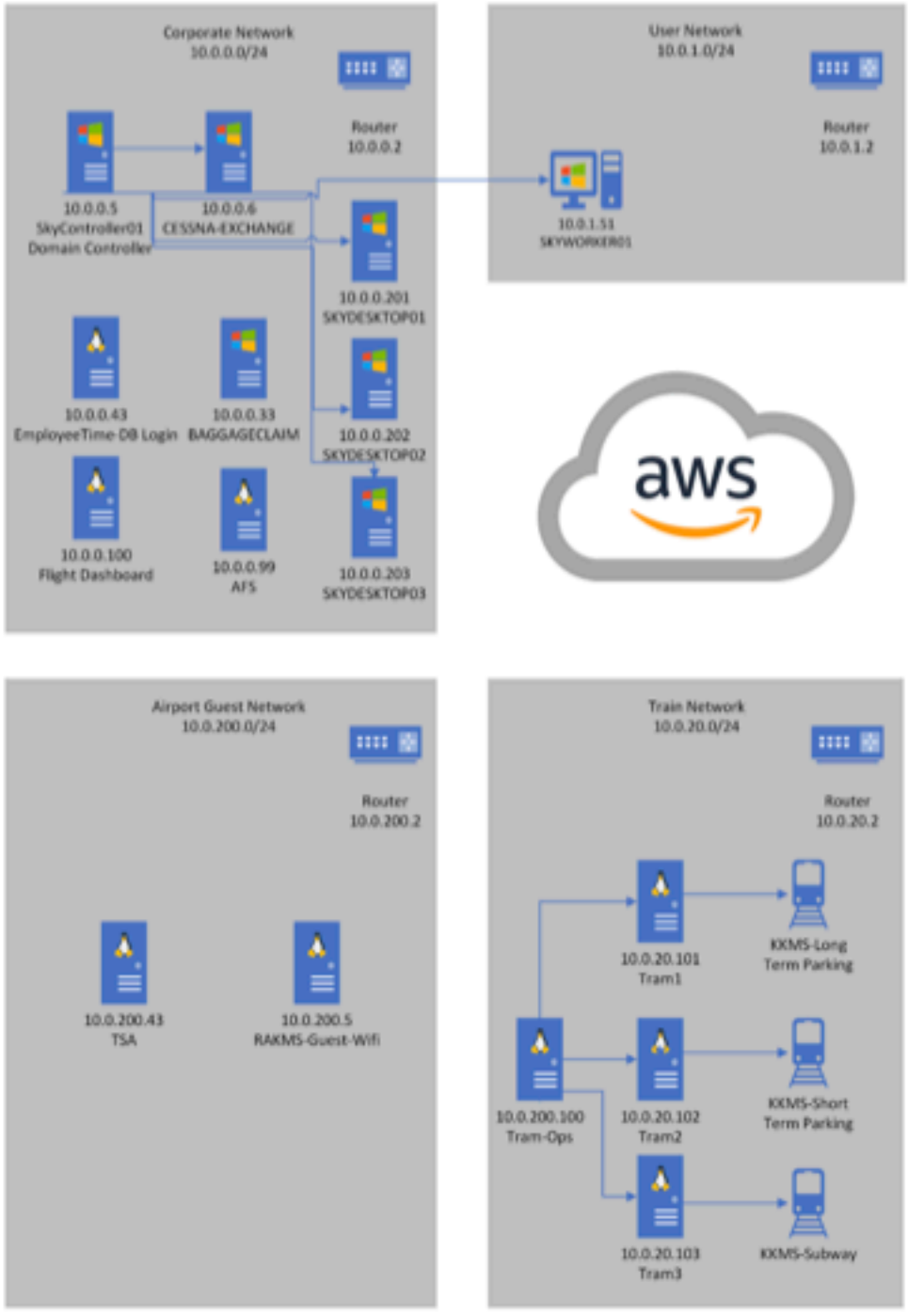
These networks were thoroughly scanned and tested for vulnerabilities that could be exploited by an attacker.

We also conducted research on publicly available information such as websites, social media, and public repositories. This information was used to gather information about the organization and identify potential vulnerabilities.

RAKMS additionally approached Finals-XX to conduct a limited-scope malicious attachment email phishing exercise against RAKMS-specified subset of employees. Phishing is a commonly used tactic by attackers to gain access to sensitive information and it was important to include it in the scope of the penetration test to ensure a thorough understanding of the organization's security posture. More information on this can be found in Appendix A - Phishing Engagement.

Network Topology

Finals-XX utilized industry-standard tools to enumerate active systems on the network. During the reconnaissance phase, Finals-XX identified 7 hosts running a Windows operating system and 6 hosts running a Linux operating system. Overall, Finals-XX discovered 16 active hosts on RAKMS' network and one AWS environment.



Testing Methodology

Penetration Testing Execution Standard

Finals-XX employs the Penetration Testing Execution Standard (PTES) as its cornerstone, ensuring a common language is shared between businesses and security service providers. This commitment to PTES allows Finals-XX to maintain a rigorous and consistent approach in all assessments, ultimately enhancing cybersecurity resilience. Through this standardized framework, Finals-XX delivers comprehensive evaluations that help clients fortify their digital defenses effectively.

Open-Source Intelligence Gathering

Finals-XX employs an Open Source Intelligence (OSINT) methodology rooted in the Open Web Application Security Project (OWASP) research. This 4-step process involves identifying information sources, collecting and processing data, ultimately yielding valuable insights for penetration testing. The analysis results guide Finals-XX during the test phase, ensuring an effective approach to network and system evaluation.

OWASP Top 10

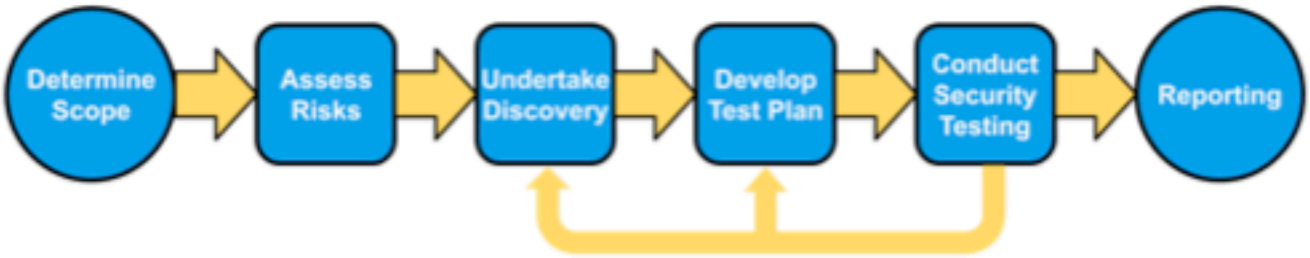
Finals-XX utilizes the Open Web Application Security Project (OWASP) Top 10 as a foundational reference for evaluating web applications in terms of common vulnerabilities and misconfigurations. OWASP's primary objective is to establish a collective understanding among web application security specialists regarding the

prevailing vulnerabilities found in contemporary applications. The 2021 edition of OWASP Top 10 identifies the following web application security weaknesses:

OWASP Top 10	
1) Broken Access Control	6) Vulnerable and Outdated Components
2) Cryptographic Failures	7) Identification and Authentication Failures
3) Injection	8) Software and Data Integrity Failures
4) Insecure Design	9) Security Logging and Monitoring Failures
5) Security Misconfiguration	10) Server-Side Request Forgery

Industrial Control Systems Security Assurance

Finals-XX follows the NIST SP 800-82 Rev. 3 Guide to Operational Technology (OT) Security as a cornerstone of our approach to assessing ICS devices and systems. This comprehensive guide provides Finals-XX with a structured framework for evaluating the security posture of Industrial Control Systems, ensuring that we adhere to industry best practices and standards.



Classification Definitions

Risk Classifications

For the technical assessment of a vulnerability, Finals-XX uses the Common Vulnerability Scoring System version 4.0 (CVSS v4.0). CVSS is a universally accepted and open standard created by the National Institute of Standards and Technology (NIST) Computer Security Resource Center (CSRC). CVSS measures a vulnerability's complexity, accessibility, and impact on the confidentiality, integrity, and availability

of a system. For the calculation of CVSS, Finals-XX utilizes the National Vulnerability Database (NVD)'s CVSS v4.0 calculator.

The scores represented in the report are based on the collective experience of Finals-XX and are tailored specifically to RAKMS. These scores are not representative of the scoring assigned officially in the NVD and should not be interpreted as such. In each vulnerability or finding table, the CVSS string is included along with the raw score to give further context to RAKMS' technical staff.

For an in-depth breakdown on the RIsk Classification scales and recommended patch lifecycles, consult Appendix A.

Level	Score
Critical	9.0-10.0
High	7.0-8.9
Medium	4.0-6.9
Low	1.0-3.9
Informational	0.0-0.9

Attack Narrative

The "Attack Narrative" refers to a chronological account of the cyber-attack, providing a comprehensive storyline that outlines the techniques, tools, and methodologies employed by the penetration testing team to exploit vulnerabilities within the target system. This narrative offers a structured overview of the team actions during the penetration test.

Day 1 - 1/12/24

Time	Notes
9:30 AM	• Engagement begins • Access to Windows and Kali machines
10:00 AM	• Initial, fast network scans • Installing tools
10:30 AM	• Vishing phone call • Deeper network scans • Initial look at websites that showed in network scans • Nmap aggregator setup
11:00 AM	• Ran vulnerability scan of Corporate network • Tried exploits the worked on past penetration test • AWS access acquired by email • Train APIs moved to train network
11:30 AM	• AWS research and initial searching • Lockout of Domain Admin account • Continued reconnaissance on network • Prowler Scan ran on AWS
12:00 AM	• Ran vulnerability scan on Airport Guest network • Request for Threat Prioritization Assessment on Top 5 threats for Robert Kalka • SOC Team informed us of account lockout, follow up email explaining the situation was sent • Directory busting websites
1:00 PM	• Threat Prioritization Assessment completed • Team member sent to search for radio signals • Team member returned 15 minutes later
1:30 PM	• AWS enumeration found 90+ buckets • Website cookie enumeration

2:00 PM	• Enumeration on Domain Controller using ldapsearch • Ldapsearch found username/password and PII
2:30 PM	• Enumeration with found user • Locked out user and made report • AWS Team meet with our team to answer questions • AWS Team informed us of looking for assumed roles to get further into the AWS environment
3:00 PM	• Ran tool, LinWinPwn to do Active Directory enumeration and vulnerability scanning • Found Domain Controller was vulnerable ZeroLogon • Used ZeroLogon to reset Machine Account password • Used Impacket to dump hashes
3:30 PM	• Continue with Domain Controller and AWS enumeration
5:00 PM	Day 1 ends

Day 2 - 1/13/24

Time	Notes
9:00 AM	Day 2 begins
9:30 AM	• Impacket Asrep roastable user • Ran Post-Modules on Msfconsole • Rescan of the environment • Setting up tools
10:00 AM	• Phishing email backend was setup and tested email • Phishing email was sent using IT director's email • Additional enumeration of the Train network • Enumeration of Exchange server
10:30 AM	• GPS Spoofing Assessment Proposal was requested
11:00 AM	• SOC Team came to inform us of more lockouts • After deliberation, it was determined automation tools caused the lockouts • Checking desktops available to RDP on within the Corporate network
11:30 AM	• AD CS enumeration started using certipy • Research On GPS Spoofing Proposal • Boarding Pass website enumeration

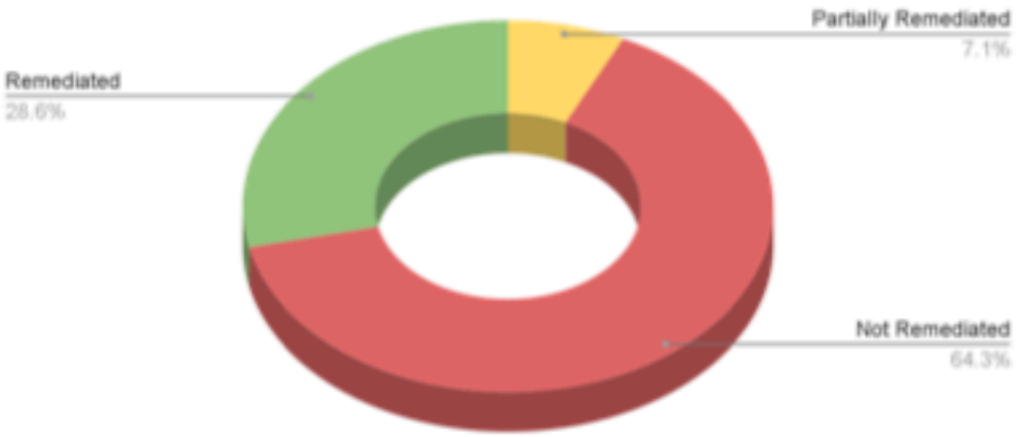
12:00 PM	• Continue work on GPS Proposal
12:30 PM	• Security team came into room and noticed an exposed password on white board • Sent GPS Spoofing Proposal document
1:00 PM	• Security team came back after team returned from lunch and informed our team that using Zerologon on the DC was reckless • Our team acquired very good advice to know what tools you are using and how it can effect what you are attacking
1:30 PM	• AI Security Presentation email received and started working on the presentation • OWASP Top 10 AI Security Issues found
2:00 PM	• Two team members sent to do Baggage Claim Radio Reverse Engineering
2:30 PM	• Continued enumeration of Corporate websites
3:00 PM	• Team members returned from Baggage Claim activity • Two Team members went to give the AI Security Presentation • Authentication bypass on AWS • Team members returned from AI Security Presentation
4:30 PM	• Team continued enumeration of websites within environment • Security Team came in during our team directory busting websites to inform us that due to the directory busting we caused a log overload
5:00 PM	• Team prepared for the finals moments by making sure every screenshot was in the right place in the one drive • Team started writing reports on findings • Team ran Openvas scan on Corporate network using Domain Credentials
5:45 PM	Engagement Ends

Reassessment Summary

During the team's previous assessment, several vulnerabilities were found. These vulnerabilities have been reassessed to test for any remediation attempted. This table shows a summary of the status of each previously discovered vulnerability.

As shown below our team was able to account for all previous findings. RAKMS shows that **64.3%** of findings was not remediated with **3** of the non-remediated findings being critical. These remediations show that RAKMS is making an effort to help secure their network.

Reassessment Pie Chart



Remediation Table

Finding Name	Risk Level	Remediation Statu
Windows Host Vulnerable to EternalRomance	Critical	Remediated
Train API Missing Access Controls	Critical	Partially Remediated
Passwords in Active Directory User Descriptions	Critical	Not Remediated
by on Rails Application Vulnerable to CVE-2019-5420	Critical	Remediated
Insecure Credentials for Timesheet Applications	Critical	Not Remediated
Missing Access Controls on Flight Dashboard	Critical	Not Remediated

Train Website Broken Access Control	**High**	Remediated
Sensitive User Data in Clear-Text	**High**	Not Remediated
AWS policy AdministratorAccess attached	**High**	Not Remediated
Any Authenticated User Can Join Hosts to Domain	**High**	Not Remediated
Ruby on Rails Webapp Vulnerable to CVE-2019-5418	**High**	Not Remediated
Insecure AWS Root Account	**High**	Not Remediated
Unauthorized Equipment Requisition System	**High**	Not Remediated
Train API accessible from Guest network	**High**	Remediated
Windows Patch levels	**Medium**	Not Remediated
No TLS on Webapps	**Medium**	Not Remediated
No Domain Account Lockout	**Medium**	Remediated
Werkzeug Debug Console enabled in production	**Medium**	Remediated
User Enumeration via Anonymous LDAP Bind	**Medium**	Not Remediated
Public Lambda functions	**Medium**	Not Remediated
SMB Signing Not Required	**Medium**	Partially Remediated
SMBv1 Enabled	**Medium**	Not Remediated
Potentially Kerberoastable User Account	**Medium**	Not Remediated
Public AWS Buckets	**Medium**	Remediated
Kerberos Preauthentication Not Required	**Medium**	Not Remediated
Website Asset Directory Traversal	**Medium**	Not Remediated
Missing "httpOnly" Cookie Attribute	**Low**	Not Remediated
Exposed Bluetooth Controls via AWS	**Low**	Remediated

Assessment Findings

Summary of Findings

Finals-XX found multiple critical vulnerabilities in RAKMS' networks, as well as server high, medium, and low severity issues which can be referenced below. We additionally detail a number of informational findings. The vulnerabilities found, when exploited, could result in loss of business operations, critical exposure of private data, and possibly loss of life.

Findings by Risk Level

Critical	High	Medium	Low	Informational
5	10	14	1	0

Table of Findings

ID	Finding	Risk Level	Risk Score (CVSSv4)
RAKMS-001	Missing Authentication on Machine Account	Critical	10.0
RAKMS-002	Zerologon - CVE-2020-1472	Critical	10.0
RAKMS-003	Overprivileged Machine Account	Critical	9.4
RAKMS-004	Missing Access Controls on Flight Dashboard	Critical	9.3
RAKMS-005	Dangerous User ACL	Critical	9.0
RAKMS-006	Insecure AWS Root Account	High	8.9
RAKMS-007	Network-Exposed Air Traffic Control Systems	High	8.9
RAKMS-008	SMTP Relay	High	8.8
RAKMS-009	Tool Requisition Auth Bypass	High	8.7
RAKMS-010	Train Website Broken Access Control	High	8.7
RAKMS-011	Insecure Credentials for Timesheet Applications	High	8.6

RAKMS-012	Passwords in Active Directory User Descriptions	High	8.5
RAKMS-013	AWS policy AdministratorAccess attached	High	7.5
RAKMS-014	Dangerous ADCS Templates	High	7.3
RAKMS-015	Kerberoastable User Account	High	7.1
RAKMS-016	Train API Unauthorized Train Registration	Medium	6.9
RAKMS-017	Exposed Debug Endpoint On Debug Server	Medium	6.9
RAKMS-018	Anonymous Bind Enabled on LDAP	Medium	6.9
RAKMS-019	ASREPRoastable User	Medium	6.9
RAKMS-020	Unauthenticated Equipment Requisition System	Medium	5.7
RAKMS-021	Train Dashboard Vulnerable to DOS	Medium	5.7
RAKMS-022	No TLS or Self-Signed Certificates on Webapps	Medium	5.7
RAKMS-023	Cross-Service Confused Deputy	Medium	5.7
RAKMS-024	Insecure Role Privleges in AWS	Medium	6.0
RAKMS-025	SMB Signing Not Required	Medium	5.6
RAKMS-026	Add-Computer Improper Permissions	Medium	5.3
RAKMS-027	Misconfigured Webroot Directory	Medium	5.1
RAKMS-028	Hard-Coded Credentials	Medium	5.1
RAKMS-029	SMBv1 Enabled	Medium	5.1
RAKMS-030	Missing "httpOnly" Cookie Attribute	Low	1.0

Critical Findings

RAKMS-001 Missing Authentication on Machine Account

The ATC-CONTROLLER-$.CORP.KKMS.LOCAL machine account doesn't require authentication, and due to RAKMS-003, it can lead to the complete exploitation of the Active Directory environment.

Affected systems

Zone	Hostname	IP
Corporate	Skycontrol01	10.0.0.5

Vulnerability Scoring

Risk Assessment		CVSS v4.0 Score
Exploit Likelihood	Likely	10.0 Critical
Business Impact	High	
Remediation Difficulty	Easy	
CVSS v4.0 Vector	CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:H/VI:H/VA:H/SC:H/SI:H/SA:H	

Technical Impact

The ATC-CONTROLLER-$.CORP.KKMS.LOCAL machine account doesn't require authentication, and due to RAKMS-003, it can easily lead to an attacker obtaining Domain/Enterprise administrator on the active directory environment. An attacker could abuse this access to obtain sensitive information and provide high enough permissions to change records, data, and permissions.

Business and Compliance Impact

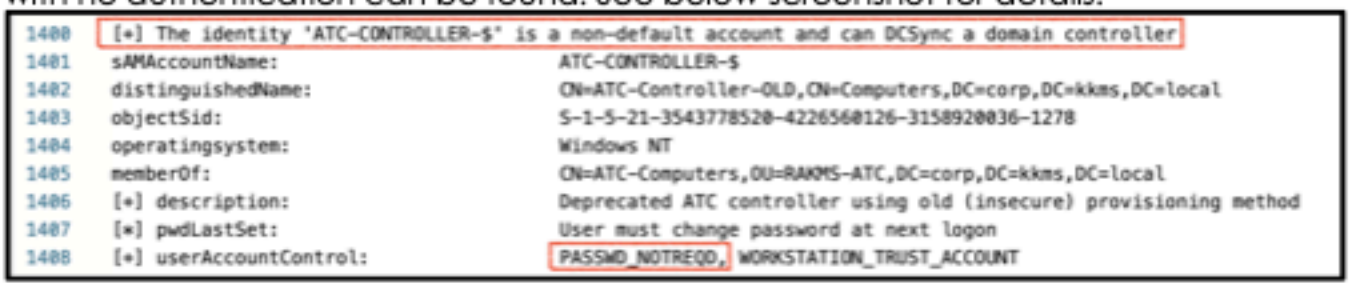
This machine account could lead to an attacker significantly disrupting business operations, potentially leading to a complete shutdown of all company operations, costing RAKMS significantly. This finding also opens RAKMS to regulatory fines, as complete access to the active directory environment can allow an attacker to obtain emails, PII, and more. The finding can also incur legal costs and liability due to significant disruption of airport operations.

Remediation:

We recommend disabling and removing the ATC-CONTROLLER-$.CORP.KKMS.LOCAL machine account. This would remove an incredibly risky attack chain.

Steps to reproduce

By leveraging a vulnerability auditing tool such as winPEAS-NG, machine accounts with no authentication can be found. See below screenshot for details.



winPEAS showing the ATC-CONTROLLER-$ userAccountControl

ATC-CONTROLLER-$ without a password

Reference(s):

- https://specopssoft.com/blog/find-ad-accounts-using-password-not-required-blank-password/

RAKMS-002 Zerologon - CVE-2020-1472

The Zerologon vulnerability is named for a flaw in the Windows login that allows for a takeover of the system account. This vulnerability is deemed critical due to its severity.

Affected systems

Zone	Hostname	IP
Corporate	Skycontrol01	10.0.0.5

Vulnerability Scoring

Risk Assessment		CVSS v4.0 Score
Exploit Likelihood	Likely	10.0 Critical
Business Impact	High	
Remediation Difficulty	Easy	
CVSS v4.0 Vector	CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:H/VI:H/VA:H/SC:H/SI:H/SA:H	

Technical Impact

This vulnerability allows for the takeover of the NT Authority\System account due to it exploiting a flaw in the Windows logon process that, when leveraged, will set the accounts password to a blank one instead. Since this is on a Domain Controller, this issue goes from being system-wide to Network-wide with the ability to access Domain Resources.

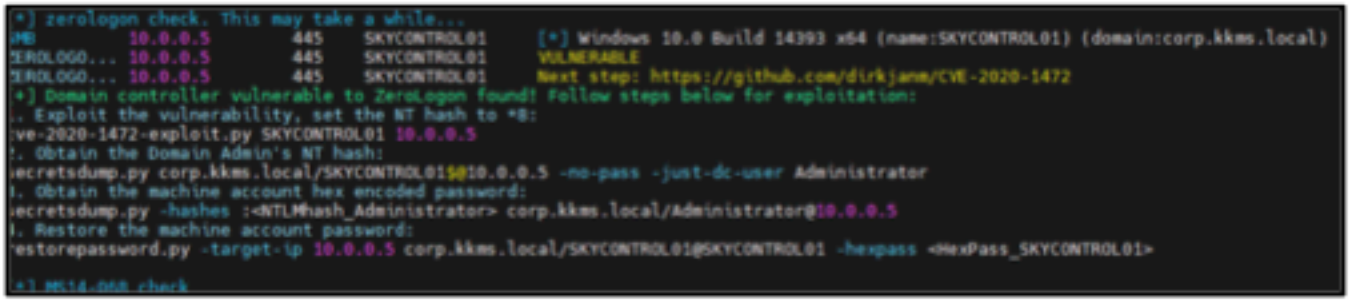
Business and Compliance Impact

This finding violates several industry security standards, implicating hefty fines. If unpatched, a malicious actor could fully compromise the entire domain and do potentially irreparable damage. This would lead to fines, damage to the company's image, and the extremely likely chance of leaking confidential company data.

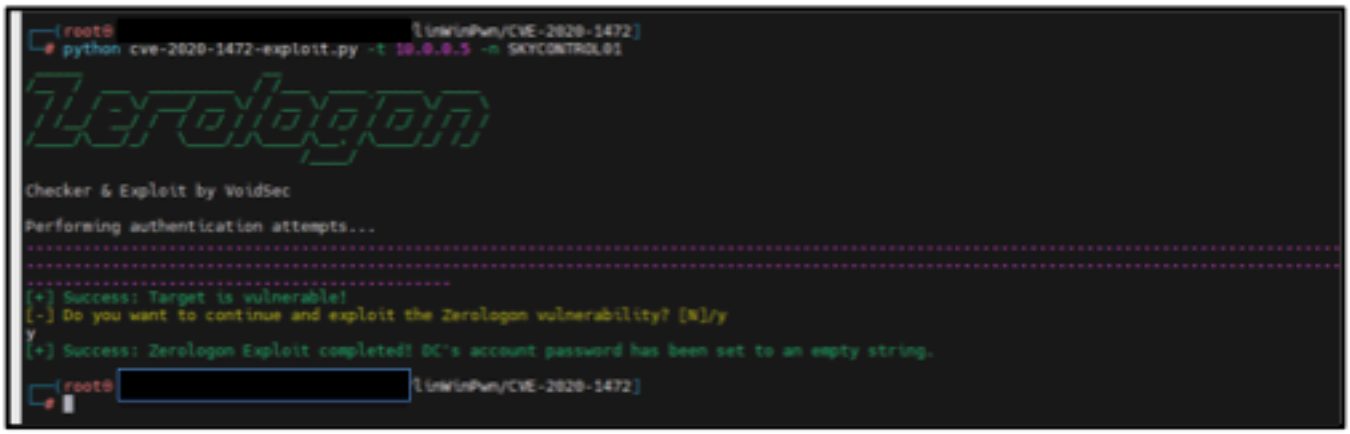
Remediation

To remediate this critical finding, we recommend updating the system or altering a registry key to mitigate the attack.

Steps to reproduce



Team tooling showing the domain controller is vulnerable to ZeroLogon and being exploited



ZeroLogon being exploited by metasploit

Using an enumeration tool such as LinWinPwn (as used in the first screenshot), the user can learn that the system is vulnerable. From there, the user can either search for it using the Metasploit framework or pull down a PoC from the internet and run it. The specific script used by the team is linked as a reference.

Reference(s):

- https://www.crowdstrike.com/blog/cve-2020-1472-zerologon-security-advisory/
- https://nvd.nist.gov/vuln/detail/cve-2020-1472
- https://github.com/dirkjanm/CVE-2020-1472

RAKMS-003 Overprivileged Machine Account

The ATC-CONTROLLER-$.CORP.KKMS.LOCAL machine account has DCsync permissions, allowing it to be exploited to create a domain controller and obtain full access to the active directory environment by a malicious attacker.

Affected systems

Zone	Hostname	IP
Corporate	Skycontrol01	10.0.0.5

Vulnerability Scoring

Risk Assessment		CVSS v4.0 Score
Exploit Likelihood	Likely	9.4 Critical
Business Impact	High	
Remediation Difficulty	Easy	
CVSS v4.0 Vector	CVSS:4.0/AV:N/AC:L/AT:N/PR:L/UI:N/VC:H/VI:H/VA:H/SC:H/SI:H/SA:H	

Technical Impact

If an attacker gains access to a machine account, either through a vulnerable service or misconfiguration, they would be able to escalate to domain admin.

Business and Compliance Impact

Overprivileged machine accounts can be utilized to turn a relatively minor vulnerability in a service into a severe threat to the entire environment, providing an entry point for an attacker to gain full control of every domain joined system on the network.

Remediation:

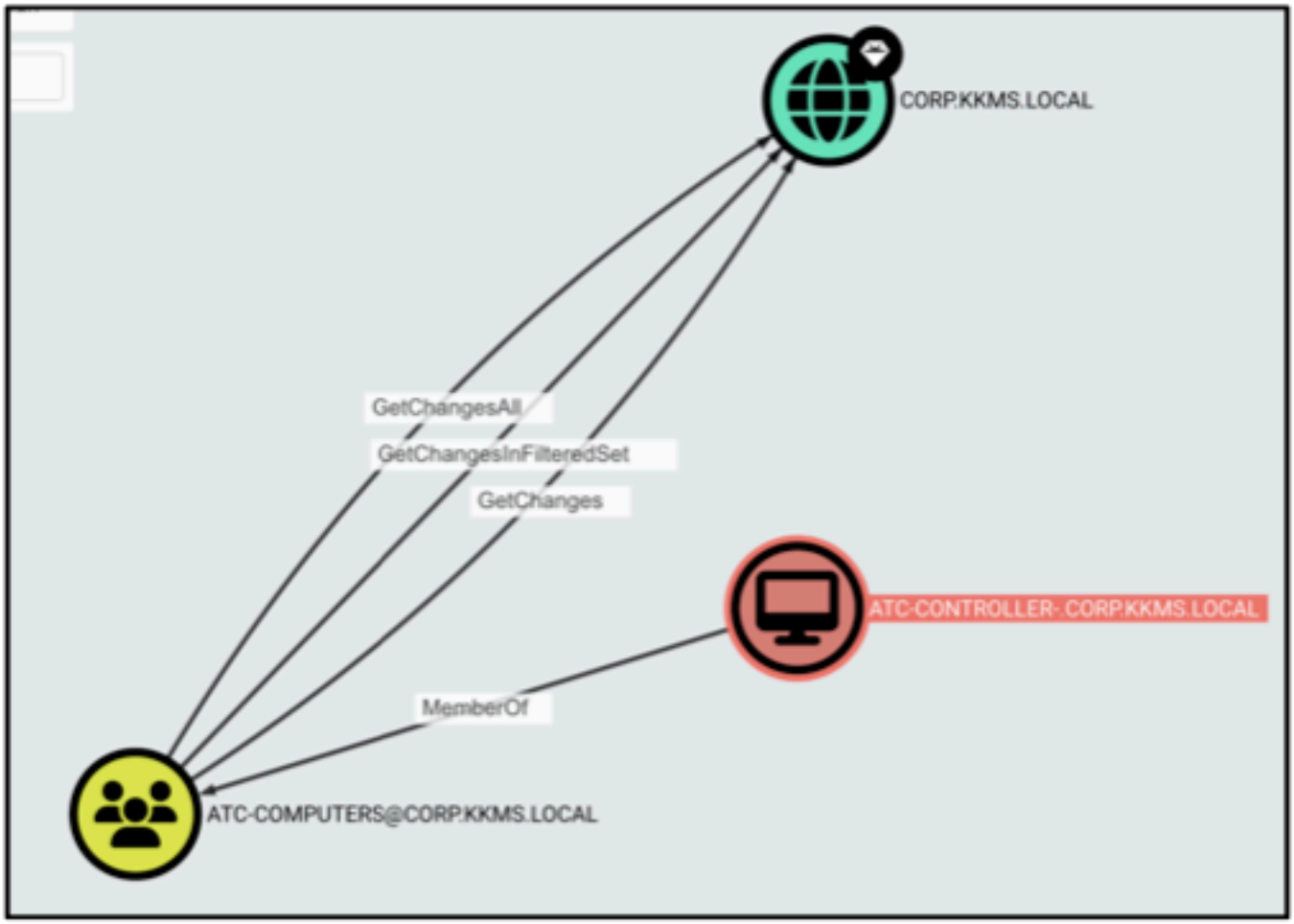
Deprivileging or removing the The ATC-CONTROLLER-$.CORP.KKMS.LOCAL machine account would remove the ability for an attacker to abuse in order to obtain domain admin.

Steps to reproduce

By leveraging a vulnerability auditing tool such as winPEAS-NG, overprivileged machine accounts can be found. See below screenshot for details.

```
1400  [+] The identity 'ATC-CONTROLLER-$' is a non-default account and can DCSync a domain controller
1401  sAMAccountName:                ATC-CONTROLLER-$
1402  distinguishedName:             CN=ATC-Controller-OLD,CN=Computers,DC=corp,DC=kkms,DC=local
1403  objectSid:                     S-1-5-21-3543778520-4226560126-3158920036-1278
1404  operatingsystem:               Windows NT
1405  memberOf:                      CN=ATC-Computers,OU=RAKMS-ATC,DC=corp,DC=kkms,DC=local
1406  [+] description:               Deprecated ATC controller using old (insecure) provisioning method
1407  [+] pwdLastSet:                User must change password at next logon
1408  [+] userAccountControl:        PASSWD_NOTREQD, WORKSTATION_TRUST_ACCOUNT
```

Winpeas output showing ATC-CONTROLLER-$ user having permission to become a domain controller.



Bloodhound showing how ATC-CONTROLLER-$ would be able to gain domain admin

Reference(s):

- https://book.hacktricks.xyz/windows-hardening/active-directory-methodology/dcsync

RAKMS-004 Missing Access Controls on Flight Dashboard

The corporate flight list web page allows unauthenticated users to freely add and delete flight listings, potentially compromising the integrity and privacy of the system's data.

Affected systems

Zone	Hostnames	IPs
Train	tram-ops	10.0.20.100

Vulnerability Scoring

Risk Assessment		CVSS v4.0 Score
Exploit Likelihood	Likely	9.3 Critical
Business Impact	Critical	
Remediation Difficulty	Medium	
CVSS v4.0 Vector	CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:H/VI:H/VA:L/SC:N/SI:N/SA:N	

Technical Impact

This vulnerability allows unauthenticated users to update, delete, and create fake flight postings.

Business and Compliance Impact

The regulatory impact of allowing unauthenticated users to manipulate flight postings includes potential violations of aviation safety regulations and data security standards, leading to legal repercussions and fines. From a business perspective, it can result in reputational damage, loss of customer trust, and financial losses due to operational disruptions and potential legal actions.

Remediation

While moving the train API to the train network is a great step in the right direction, we recommend adding proper authentication methods to restrict access to the API.

Steps to reproduce

We recommend implementing proper access controls for the APIs, such as API keys, OAuth 2.0, or JWT (JSON Web Tokens).

Reference(s):

1. Run the command shown in the screenshot below

cURL command demonstrating the server responding to unauthenticated API requests

RAKMS-005 Dangerous User ACL

User 'osanders' is not a Domain Administrator but has 'writeDacl' permissions to all domain objects. This allows them to have essentially full control of the domain.

Affected systems

Zone	Hostnames	IPs
Corporate	SkyControl01	10.0.0.5

Vulnerability Scoring

Risk Assessment		CVSS v4.0 Score
Exploit Likelihood	Possible	9.0 Critical
Business Impact	Critical	
Remediation Difficulty	Medium	
CVSS v4.0 Vector	CVSS:4.0/AV:N/AC:H/AT:P/PR:L/UI:N/VC:H/VI:H/VA:H/SC:H/SI:H/SA:H	

Technical Impact

Granting 'writeDacl' permissions to a non-Domain Administrator like 'osanders' poses significant security risks, as it allows them to modify access controls across the entire domain without the typical oversight afforded to Domain Administrators. This capability can lead to unauthorized access, manipulation of security settings, and potential breaches, effectively providing 'osanders' with full control over the domain. Such a setup violates the principle of least privilege and complicates tracking and auditing of changes, increasing the risk of both deliberate and accidental misuse of these extensive permissions.

Business and Compliance Impact

'writeDacl' permissions to a non-Domain Administrator such as 'osanders' has serious business and compliance implications. This configuration increases the risk of data breaches and unauthorized access, potentially leading to significant financial losses, damage to the organization's reputation, and erosion of customer trust. From a compliance standpoint, it violates the principle of least privilege, a fundamental requirement in many regulatory frameworks, exposing the organization to legal penalties and non-compliance issues with standards like GDPR or PCI-DSS. Such a

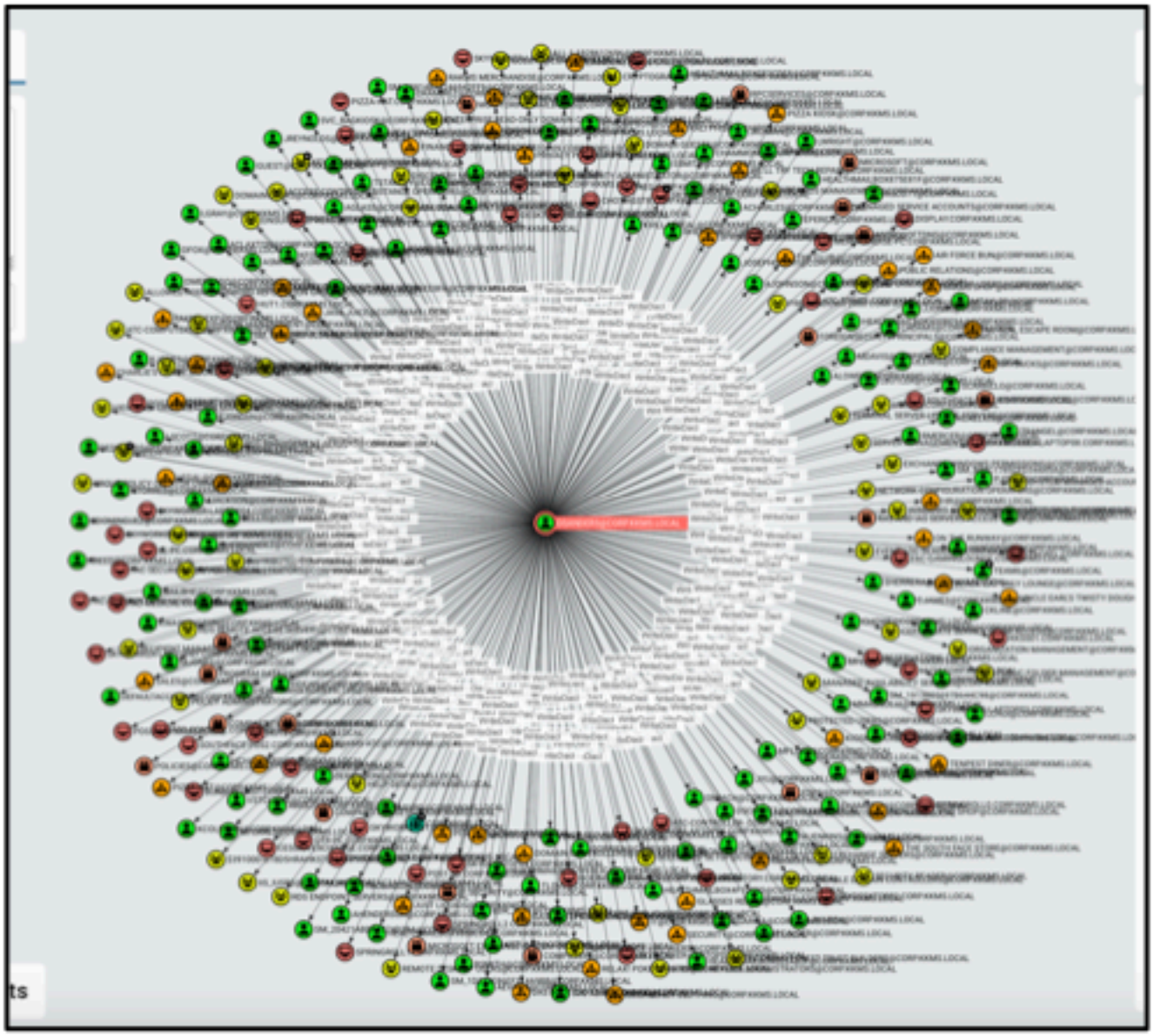
setup could also result in increased audit costs and insurance premiums due to the heightened risk profile.

Remediation

We recommend you remove the extended ACL permissions from 'osanders'

Steps to reproduce

1. Audit the permissions of users in the environment using a tool such as WinPeas or BloodHound.



Objects osanders has permissions to modify (image via Bloodhound)

Reference(s):

- https://stealthbits.com/blog/active-directory-permissions-hiding-in-the-shadows/

High Findings

RAKMS-006 Insecure AWS Root Account

The Root AWS account has multiple misconfigurations, including lack of MFA, access key enabled, and other minor misconfigurations.

Affected systems

Zone
AWS

Vulnerability Scoring

Risk Assessment		CVSS v4.0 Score
Exploit Likelihood	Unlikely	8.9 High
Business Impact	Severe	
Remediation Difficulty	Medium	
CVSS v4.0 Vector	CVSS:4.0/AV:N/AC:H/AT:P/PR:H/UI:N/VC:H/VI:H/VA:H/SC:H/SI:H/SA:H	

Technical Impact

The root account is the most privileged user in an AWS account. This should be locked down and not used if possible. The lack of protective guards adds to the risk of compromise to the root account and, by extension, the entire AWS environment.

Business and Compliance Impact

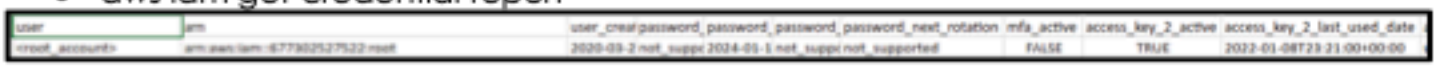
The misconfigurations in the root AWS account represent a compliance issue as they do not adequately secure access to critical cyber systems, potentially allowing unauthorized entry.

Remediation

We recommend implementing hardware MFA, revoking access keys to the root account, and implementing role-based accounts that follow the principal of least privilege.

Steps to Reproduce

- Configure the aws-cli config with the user's access keys
- aws iam generate-credential-report
- aws iam get-credential-report



user	arn	user_creat	password_	password_	password_	password_next_rotation	mfa_active	access_key_2_active	access_key_2_last_used_date
<root_account>	arn:aws:iam::677302527522:root	2020-03-2	not_suppo	2024-01-1	not_suppo	not_supported	FALSE	TRUE	2022-01-08T23:21:00+00:00

Report showing no MFA

Reference(s):

- https://docs.aws.amazon.com/cli/latest/reference/iam/
- https://docs.aws.amazon.com/SetUp/latest/UserGuide/best-practices-root-user.html
- https://docs.aws.amazon.com/wellarchitected/latest/security-pillar/sec_securely_operate_aws_account.html

RAKMS-007 Network-Exposed Air Traffic Control Systems

ATC-Control and ATC-Tower were both domain-joined to corp.kkms.local. This means that an attacker that gains access to the domain would be able to log in to devices within the Air Traffic Control Tower, which should be a highly secure zone, isolated from the rest of the network.

Affected systems

Zone	Hostnames
User	ATC-Control ATC-Tower

Vulnerability Scoring

Risk Assessment		CVSS v4.0 Score
Exploit Likelihood	Possible	8.9 High
Business Impact	Critical	
Remediation Difficulty	Medium	
CVSS v4.0 Vector	CVSS:4.0/AV:N/AC:H/AT:N/PR:H/UI:N/VC:H/VI:H/VA:H/SC:H/SI:H/SA:H	

Technical Impact

Without network segmentation, a breach of the active directory domain could allow an attacker access to air traffic control systems. An attacker could disrupt critical business and safety systems and could cause irreparable damage to both infrastructure and data.

Business and Compliance Impact

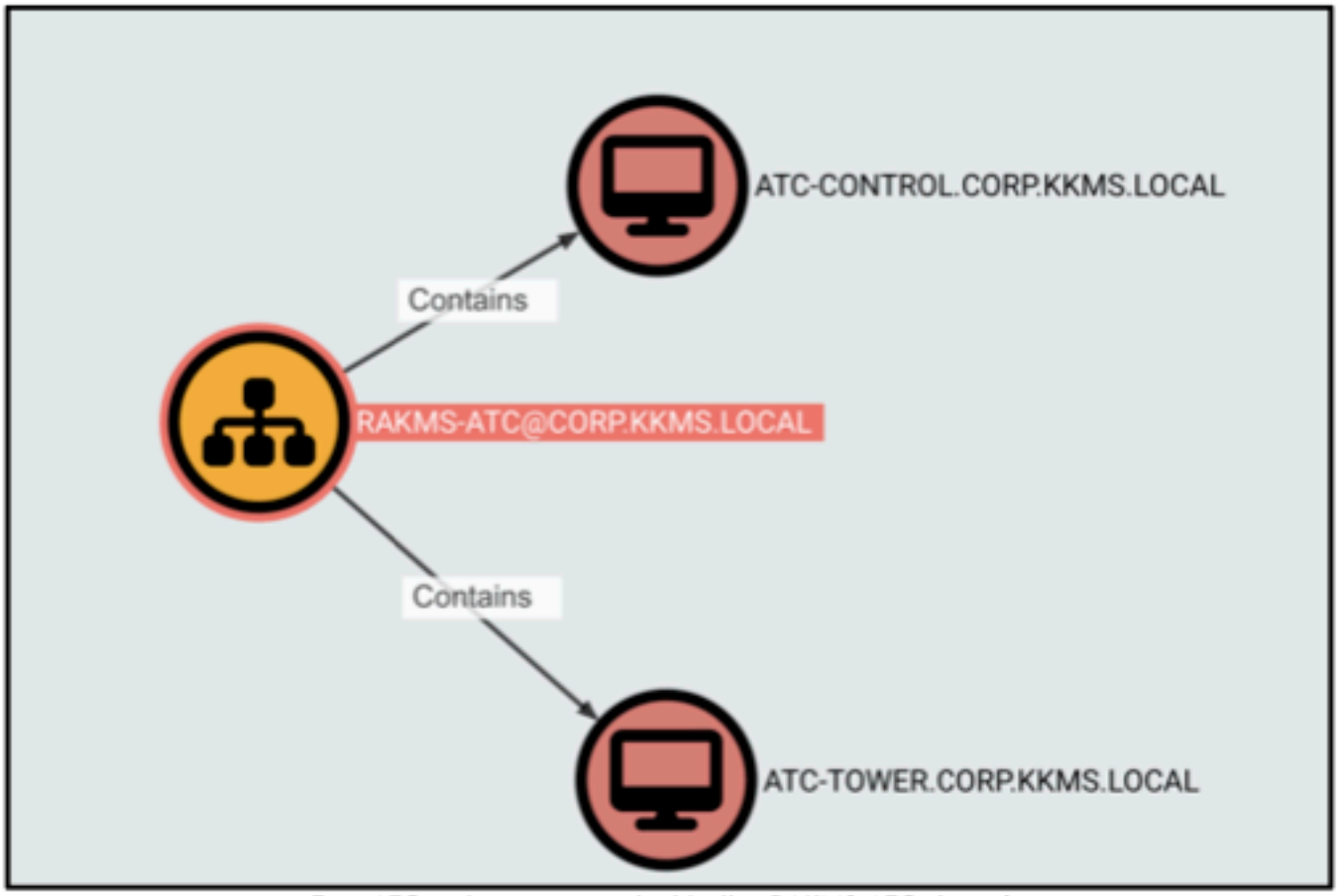
The presence of a network connected air traffic controller can impact the ability of the business to safely conduct air traffic in a safe manor. This is also in violation of TSA Cybersecurity Directives, which can lead to heavy fine

Remediation

We recommend segmenting the air traffic control tower systems from the rest of the network, mitigating the risk of exploitation through the active directory domain, and aligning RAKMS with TSA Cybersecurity guidelines.

Steps to reproduce

Using an active directory attack chain enumeration tool like bloodhound, attack chains can be visualized toward systems within an active directory domain.



Two ATC systems connected to the RAKMS-ATC domain group

Reference(s):

- https://www.prnewswire.com/news-releases/tsa-issues-new-cybersecurity-requirements-for-airport-and-aircraft-operators-301765090.html
- https://www.vmware.com/topics/glossary/content/network-segmentation.html#:~:text=Network%20segmentation%20is%20a%20network,services%20to%20each%20sub%2Dnetwork.

RAKMS-008 SMTP Relay

The exchange server on 10.0.0.6 allows relays from any user that can be sent from any email without authentication or verification.

Affected systems

Zone	Hostnames	IPs
Corporate	CESSNA-EXCHANGE	10.0.0.6

Vulnerability Scoring

Risk Assessment		CVSS v4.0 Score
Exploit Likelihood	Possible	8.8 High
Business Impact	Critical	
Remediation Difficulty	Medium	
CVSS v4.0 Vector	CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:L/VI:H/VA:N/SC:N/SI:N/SA:N	

Technical Impact

Any threat actor with access to the network can utilize this to impersonate any email and make phishing attempts and other mail abuses look legitimate. This can lead to countless Social Engineering attacks that will be extremely successful. Depending on who is breached, the entire domain can easily be compromised with only a command or two run on the network without any need for credentials or other permissions.

Business and Compliance Impact

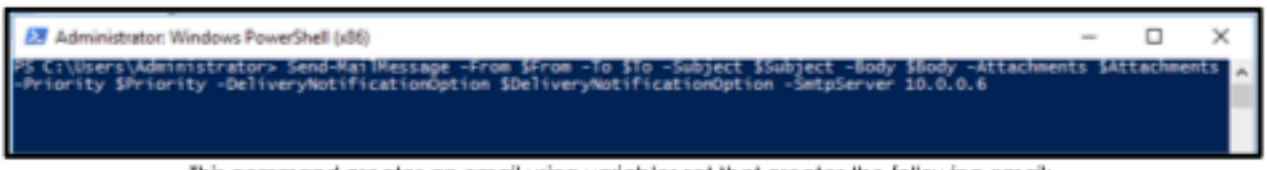
Compromises of this nature will lead to countless losses for the business in time and money. Customer trust will erode, and employee productivity will deteriorate due to the complications this vulnerability will have on their workflows. This vulnerability will also cause many penalties in the various compliance standards, such as the GDPR and others that RAKMS must be compliant with.

Remediation

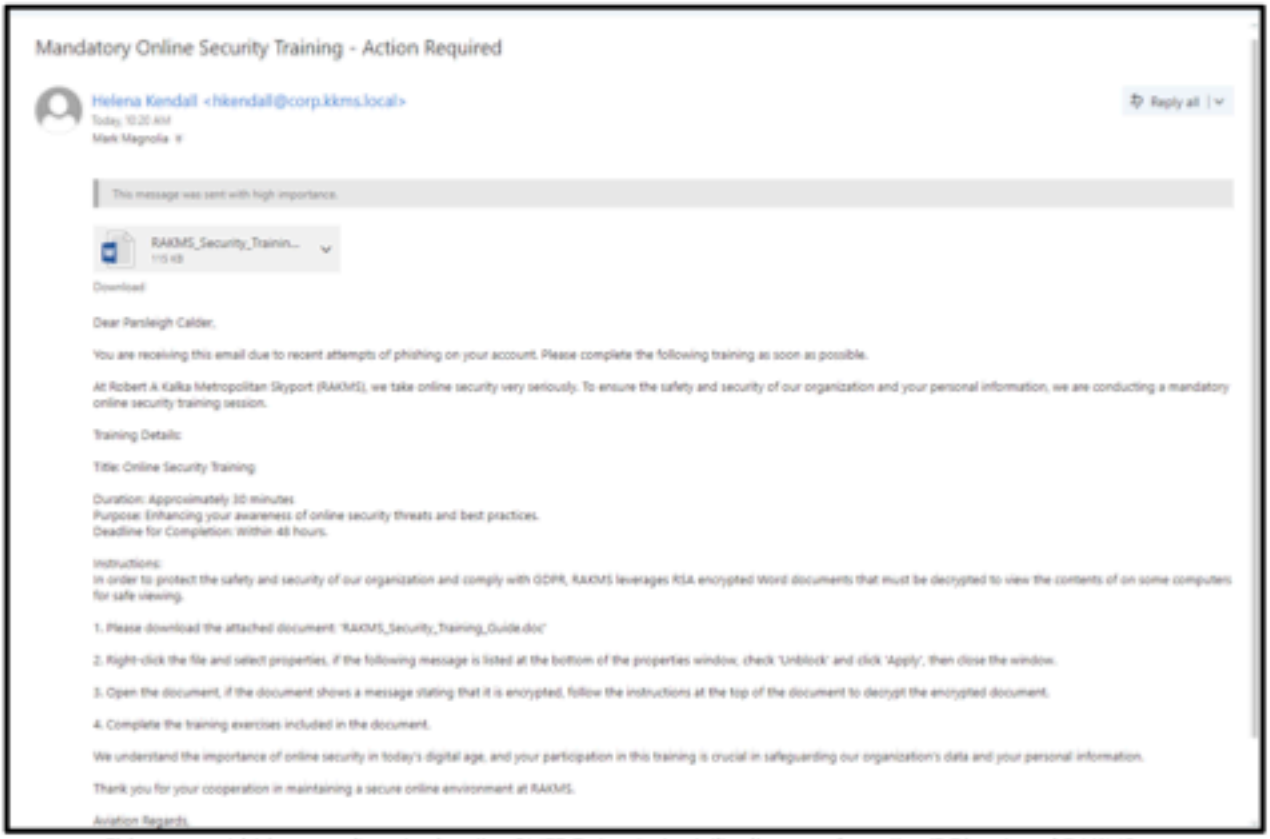
We recommend implementing technologies such as DMARC, DKIM, and SPF that will verify senders as legitimate.

Steps to reproduce

1. Write a PowerShell command to write your email as whoever you want without verification and use SMTP Relay through 10.0.0.6.



This command creates an email using variables set that creates the following email:



This was a phishing email sent using the SMTP Relay to look like it came from the IT Director of RAKMS

Reference(s):

- https://learn.microsoft.com/en-us/powershell/module/microsoft.powershell.utility/send-mailmessage?view=powershell-7.4
- https://cp.tc/blog/suu0lwzeafo8q97p8teu0nffointmw

RAKMS-009 Tool Requisition Auth Bypass

Local authentication vulnerability allows large company purchases using the tool requisition page to bypass facial recognition authentication.

Affected systems

Zone	Endpoint
AWS	http://rakmstoolrequisition20240111034801124200000007.s3-website-us-east-1.amazonaws.com/

Vulnerability Scoring

Risk Assessment		CVSS v4.0 Score
Exploit Likelihood	Possible	8.7 High
Business Impact	Severe	
Remediation Difficulty	Medium	
CVSS v4.0 Vector	CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:N/VI:N/VA:H/SC:N/SI:N/SA:N	

Technical Impact

This vulnerability would allow anyone in the world to purchase tools at the company's expense, resulting in undefined losses to company revenue.

Business and Compliance Impact

If abused, this vulnerability would lead to an undefined loss in company revenue. The company would take a massive hit to its reputation by allowing unauthorized purchases like this.

Remediation

Client-side authentication is considered very poor practice and we do not recommend it it any situation. We recommend adding a server-side login to the order portal and hosting the application locally to reduce the attack surface.

Steps to reproduce

1. Since the authentication is client-side, you can modify the API response to not ask for facial recognition.

```
> tool=JSON.parse(resp)
◂ ▸ {tool: {…}, req: {…}}
> tool.req.authRequired=false
◂ false
> resp=JSON.stringify(tool)
◂ '{"tool":{"itemDesc":{"S":"Milwaukee 2606-22CT (1 EA)"},"price":{"N":"261.55"},"nam
  e":{"S":"Power Drill"},"weight":{"N":"3.31"}},"req":{"reqID":{"S":"206213"},"itemNam
  e":{"S":"Power Drill"},"itemCost":{"N":"261.55"},"authRequired":false,"finalQuantit
  y":{"N":"0"},"orderPushed":{"BOOL":false}}}'
```

Firefox debug console changing authRequired to false to bypass auth

Tool requisition form with an expensive item not asking for auth.

Reference(s):

- https://owasp.org/Top10/A01_2021-Broken_Access_Control/

RAKMS-010 Train Website Broken Access Control

In the train network, three websites are accessible that display the current positions of the three trains along their lines. These services are vulnerable to an authentication bypass which grants an attacker full control of the trains, including the ability to start and stop them remotely.

Affected systems

Zone	Hostnames	IPs
Train	Tram1 Tram2 Tram3	10.0.20.101 10.0.20.102 10.0.20.103

Vulnerability Scoring

Risk Assessment		CVSS v4.0 Score
Exploit Likelihood	Possible	8.7 High
Business Impact	Critical	
Remediation Difficulty	Medium	
CVSS v4.0 Vector	CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:N/VI:N/VA:H/SC:N/SI:N/SA:N	

Technical Impact

A threat actor could use this to have complete control over any train in the network, including the ability to start and stop any train.

Business and Compliance Impact

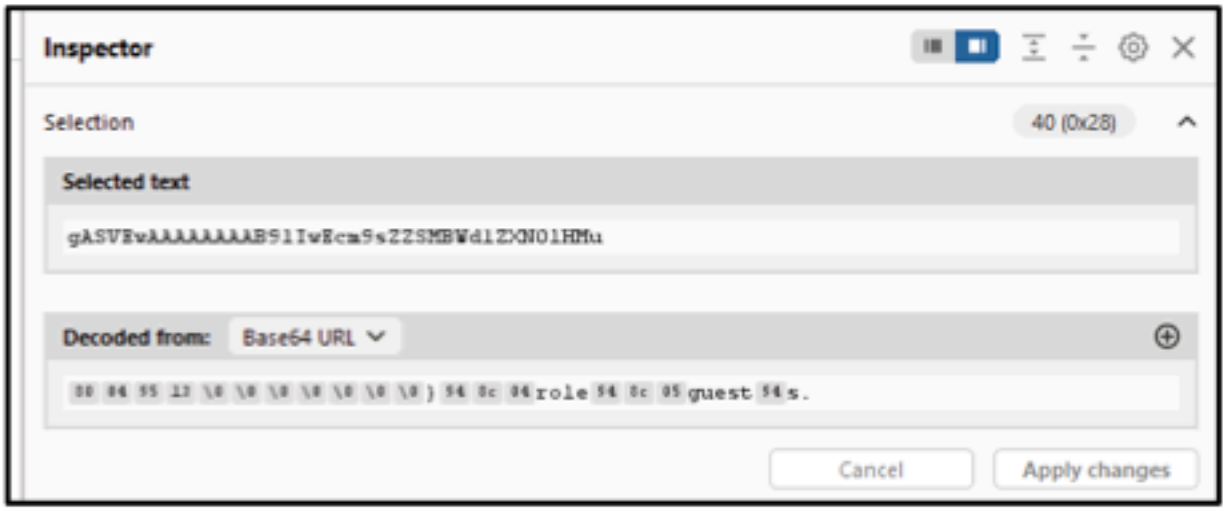
This impacts the RAKMS' ability to transport people throughout the Airport and fails to adhere to TSA guidelines on proper access controls of operational technology.

Remediation

We recommend removing the train control endpoints from an otherwise purely informational API. We recommend refactoring the authentication system to use server-side authentication instead of relying on client-side cookies as an alternative remediation strategy.

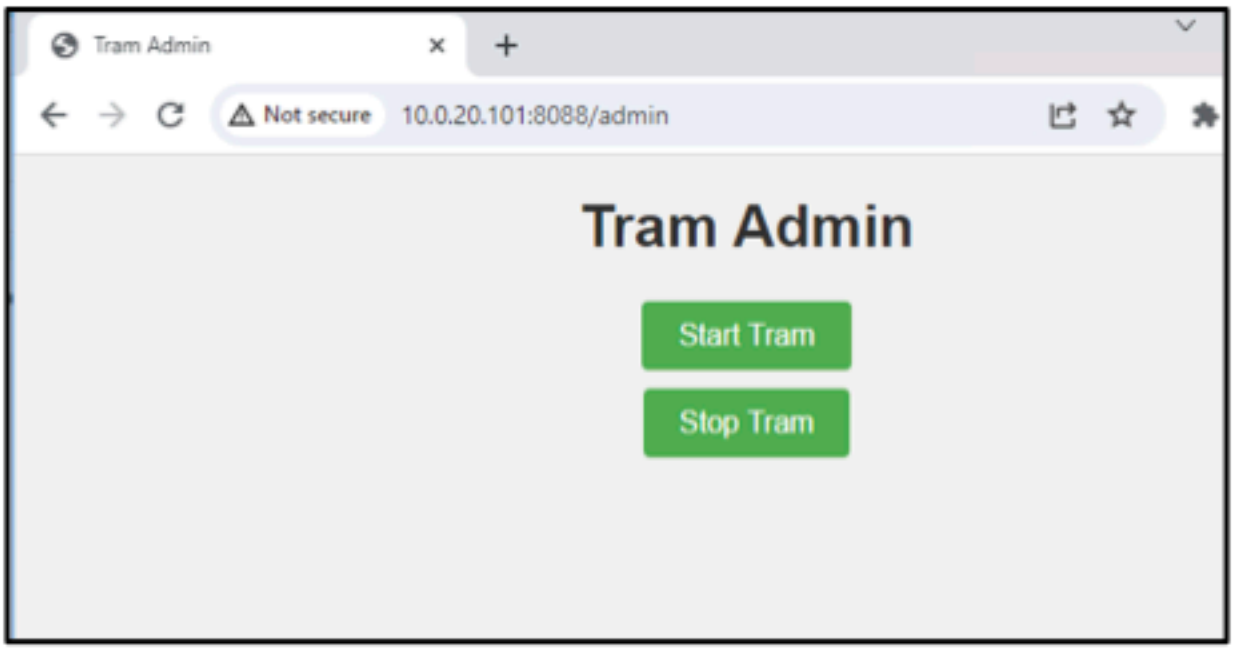
Steps to reproduce

1. Go to 10.0.20.101:8088/admin and intercept the request using BurpSuite (this works for .102 and .103 as well)
2. Decode the cookie from Base64 URL



Cookie decoded from Base64 URL

3. Change 'guest' to 'admin' and forward the request



Train admin page

Reference(s):

- https://owasp.org/Top10/A01_2021-Broken_Access_Control/

RAKMS-011 Insecure Credentials for Timesheet Applications

The web application used for timekeeping for employees on the corporate network uses weak and insecure credentials. Administrative access to the web application can be gained through the use of the username and password of "admin:admin." This combination is a commonly guessed credential pairing and can easily be used by attackers to disrupt business operations.

Affected systems

Zone	Hostname	IP
Corporate	Employee-DB Login	10.0.0.43

Vulnerability Scoring

Risk Assessment		CVSS v4.0 Score
Exploit Likelihood	Likely	8.6 High
Business Impact	Severe	
Remediation Difficulty	Easy	
CVSS v4.0 Vector	CVSS:4.0/AV:A/AC:L/AT:N/PR:N/UI:N/VC:H/VI:H/VA:N/SC:N/SI:N/SA:N	

Technical Impact

This vulnerability allows anyone to edit the employee timesheet, including adding and deleting other employees' records. Resulting in a major loss in data integrity and possible loss of revenue to the company.

Business and Compliance Impact

Interruptions to payroll can frustrate employees, impact the company's reputation, and cause legal issues for RAKMS. A bad actor or disgruntled employee could misuse administrator access to maliciously change timesheets or potentially commit time theft.

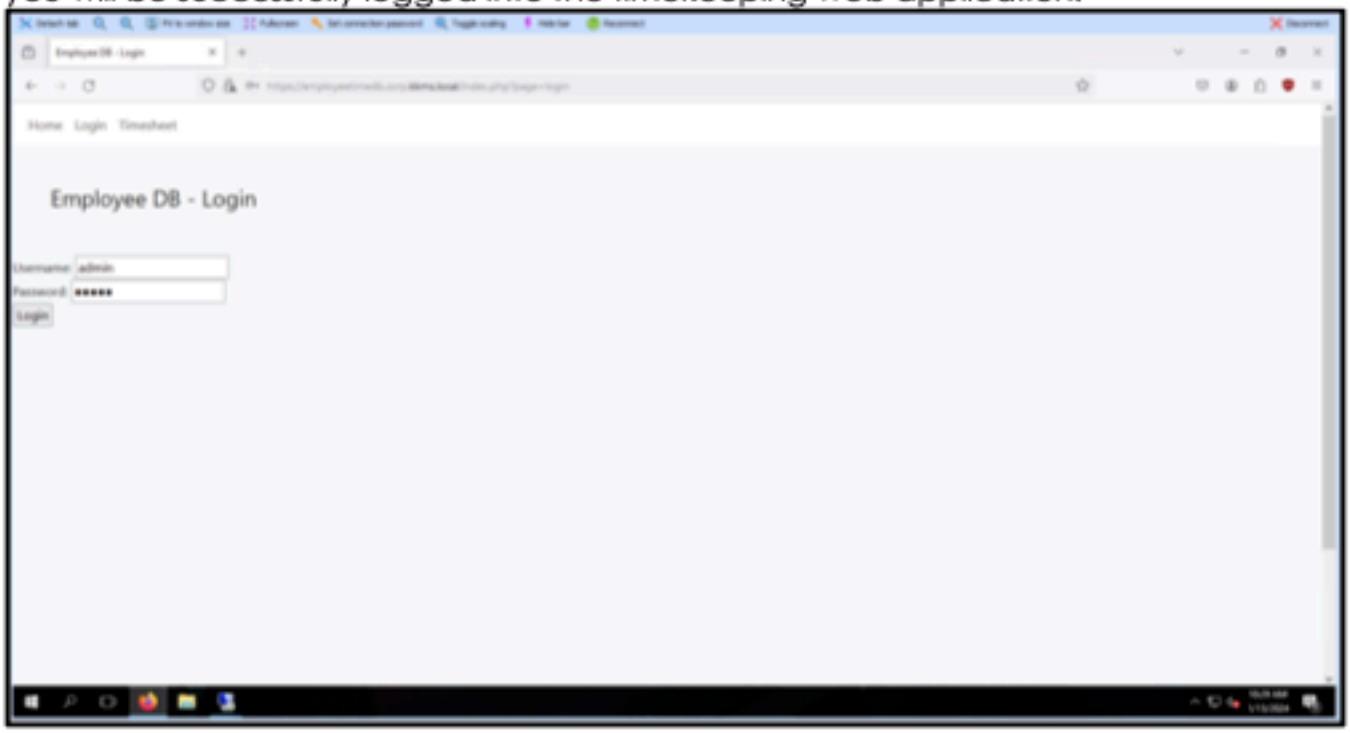
Remediation

We recommend always using secure and complex passwords to protect every administrative function, including the payroll admin account. This can be

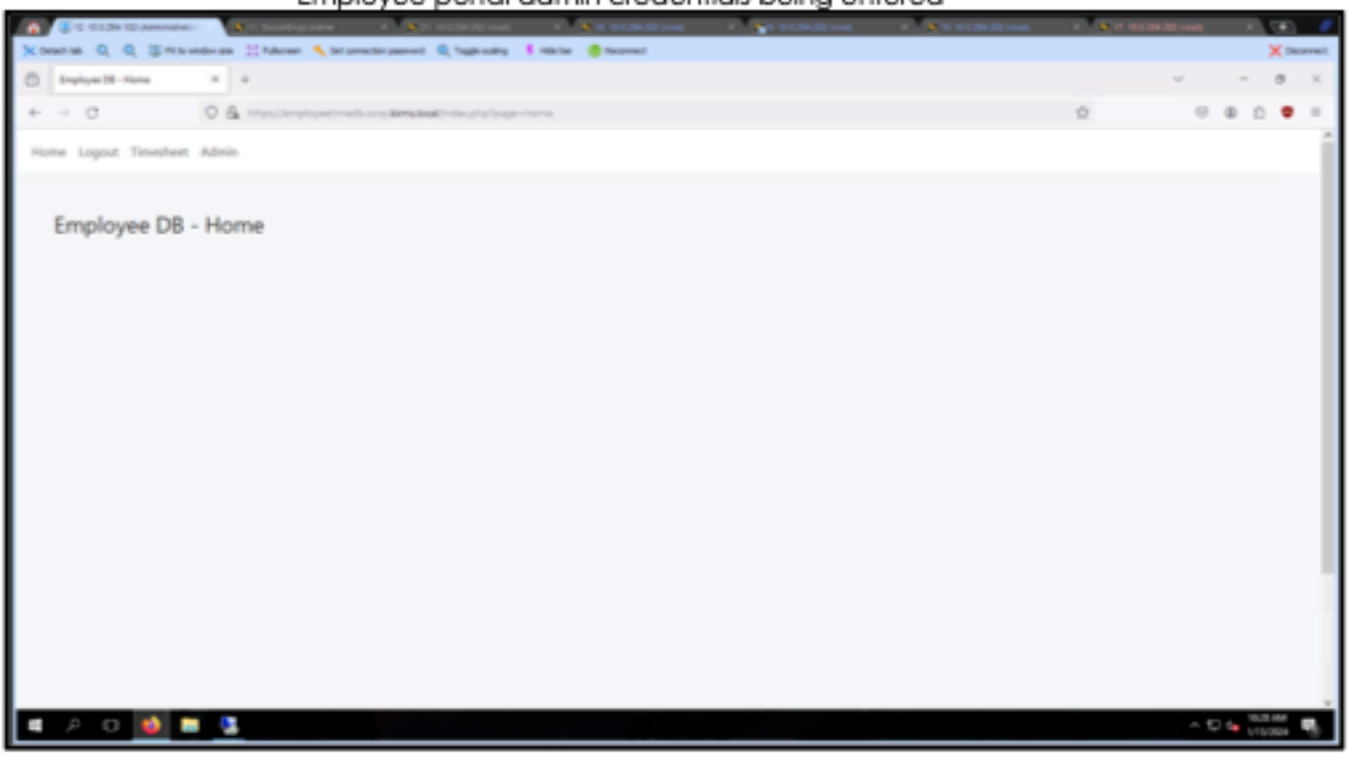
accomplished by changing the password in the admin portal to a more secure password or passphrase.

Steps to Reproduce

Go to https://employeetimedb.corp.kkms.local/index.php?page=home and enter admin:admin, which is an extremely common and insecure pair of credentials. Then, you will be successfully logged into the timekeeping web application.



Employee portal admin credentials being entered



Reference(s):

- https://cwe.mitre.org/data/definitions/1391.html

RAKMS-012 Passwords in Active Directory User Descriptions

The Active Directory user account named magnolia has a description that contains the cleartext password for the account. This password leakage, when used in conjunction with this user being configured with constrained delegation to a service account, leads to the further compromise of the associated service account, allowing escalation of privileges.

Affected systems

Zone	Hostname	IP
Corporate	SkyControl01	10.0.0.5

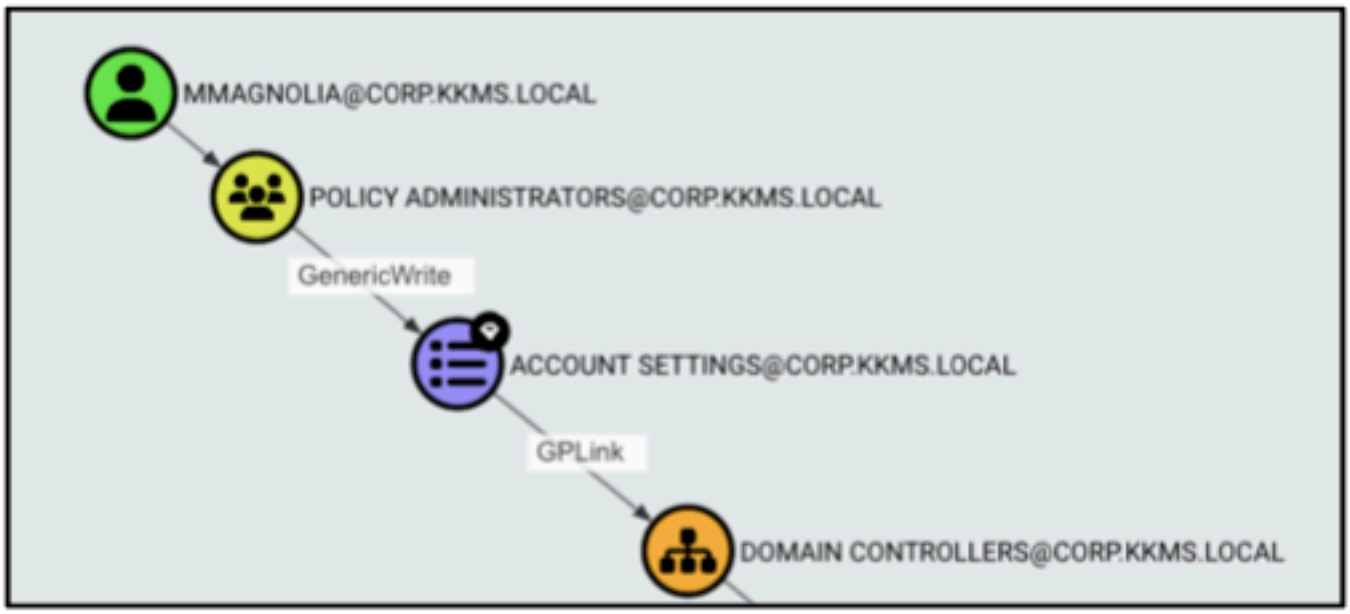
Vulnerability Scoring

Risk Assessment		CVSS v4.0 Score
Exploit Likelihood	Likely	8.5 High
Business Impact	Severe	
Remediation Difficulty	Easy	
CVSS v4.0 Vector	CVSS:4.0/AV:A/AC:L/AT:N/PR:N/UI:N/VC:H/VI:L/VA:L/SC:H/SI:L/SA:L	

Technical Impact

This allows for a compromise of the user account by anyone who is enumerating information about LDAP, which due to RAKMS-018, is possible with anonymous login.

The impact of this is increased by this account being a Policy Administrator, allowing it to modify Group Policy that is being applied to the Domain Controller. Editing this policy allows for granting access to add accounts to groups in the domain including Domain Admin.



Bloodhound showing chain from mmagnolia to Domain Controller management.

Business and Compliance Impact
Data security compliance is directly violated by having plain text credentials in any form. The leaked Active Directory passwords would significantly damage RAKMS' reputation. The lack of data security would damage customer trust and run a constant risk of downtime, data breaches, and other incidents due to the severity and simplicity of this exploit.

Remediation
We recommend that no passwords be stored in cleartext, and once the password is removed, the password gets reset.

Steps to Reproduce
By querying information from LDAP about the users, the description of mmagnolia can be found with a cleartext password.

```
cn: Mark Magnolia
sn: Magnolia
title: Manager
description: Password: [redacted]
givenName: Mark
```
Output of LDAPSearch

Reference(s):
- https://cwe.mitre.org/data/definitions/256.html

RAKMS-013 AWS policy AdministratorAccess attached

AWS policy AdministratorAccess is attached to a role and allows '*:*' administrative privileges.

Affected systems

Zone
AWS

Vulnerability Scoring

Risk Assessment		CVSS v4.0 Score
Exploit Likelihood	Unlikely	7.5 High
Business Impact	Severe	
Remediation Difficulty	Easy	
CVSS v4.0 Vector	CVSS:4.0/AV:N/AC:H/AT:P/PR:H/UI:N/VC:H/VI:H/VA:H/SC:N/SI:N/SA:N	

Technical Impact

Any user with the AdministratorAccess policy attached has full access and can delegate permissions to every service and resource in AWS. This can be used to escalate one's privileges and access confidential information.

Business and Compliance Impact

Inappropriate use or abuse of AdministratorAccess can lead to unauthorized access, data breaches, and costly security incidents, making it crucial for organizations to restrict its use to only those who require such elevated privileges for their job roles.

Remediation

It is recommended and considered a standard security advice to grant least privilege—granting only the permissions required to perform a task. Determine what users need to do and then craft policies that let them perform only those tasks instead of allowing full administrative privileges.

Steps to Reproduce

- Configure the aws-cli config with the user's access keys

- aws iam get-policy
- aws iam attach-user-policy --policy-arn arn:aws:iam:ACCOUNT-ID:aws:policy/AdministratorAccess --user-name $USER


```
        {
            "Path": "/",
            "RoleName": "AWS-QuickSetup-StackSet-Local-ExecutionRole",
            "RoleId": "AROAZ3MTAMYRNMUAHSZ4Y",
            "Arn": "arn:aws:iam::677302527522:role/
AWS-QuickSetup-StackSet-Local-ExecutionRole",
            "CreateDate": "2022-02-22T20:50:53Z",
            "AssumeRolePolicyDocument": {
                "Version": "2012-10-17",
                "Statement": [
                    {
                        "Effect": "Allow",
                        "Principal": {
                            "AWS": "arn:aws:iam::677302527522:role/
AWS-QuickSetup-StackSet-Local-AdministrationRole"
                        },
                        "Action": "sts:AssumeRole"
                    }
                ]
            },
            "InstanceProfileList": [],
            "RolePolicyList": [],
            "AttachedManagedPolicies": [
                {
                    "PolicyName": "AdministratorAccess",
                    "PolicyArn": "arn:aws:iam::aws:policy/AdministratorAccess"
                }
            ],
            "Tags": [],
            "RoleLastUsed": {}
        },
```


AdministratorAccess attached to role AWS-QuickSetup-StackSet-Local-ExecutionRole

Reference(s):

- https://docs.aws.amazon.com/cli/latest/reference/iam/
- https://docs.aws.amazon.com/IAM/latest/UserGuide/best-practices.html#grant-least-privilege
- https://docs.aws.amazon.com/cli/latest/reference/iam/get-policy.html

RAKMS-014 Dangerous ADCS Templates

The templates 'Tanium' and 'WorkstationAuthentication' are configured to permit Client Authentication, allowing users to leverage them to authenticate within the environment. In addition to this, they house the dangerous permission 'ENROLLEE_SUPPLIES_SUBJECT'. This flag enables the entity enrolling for the certificate to specify the subject name. If not properly controlled, an attacker can exploit this to

obtain a certificate with a fraudulent subject name, potentially impersonating other users or systems.

Well this vulnerability requires a machine account to exploit, RAKMS-001 and RAKMS-026 allow easy access to machine accounts.

Affected systems

Zone	Hostnames	IPs
Corporate	SkyControl01	10.0.0.5

Vulnerability Scoring

Risk Assessment		CVSS v4.0 Score
Exploit Likelihood	Possible	7.3 High
Business Impact	Critical	
Remediation Difficulty	Medium	
CVSS v4.0 Vector	CVSS:4.0/AV:N/AC:H/AT:N/PR:H/UI:N/VC:N/VI:H/VA:H/SC:H/SI:H/SA:H	

Technical Impact

An attacker exploiting this vulnerability could obtain a certificate with a fraudulent subject name. This means they could impersonate other users or systems within the network. Impersonation attacks can lead to unauthorized access to sensitive data, manipulation of system operations, and compromise system integrity.

Business and Compliance Impact

The configuration of the 'Tanium' and 'WorkstationAuthentication' templates, particularly with the 'ENROLLEE_SUPPLIES_SUBJECT' permission, poses substantial business and compliance risks. From a business perspective, the vulnerability opens doors to potential data breaches and impersonation attacks, which can disrupt operations, damage the organization's reputation, and lead to significant financial losses due to the costs associated with rectifying breaches, loss of business, and decreased customer trust. These incidents could also negatively impact future customer acquisition and partner relationships. There are compliance issues with this vulnerability as well, meaning there would be fines from governing organizations.

Remediation

To address the security concerns with the 'Tanium' and 'WorkstationAuthentication' templates, we advise removing or strictly regulating the 'ENROLLEE_SUPPLIES_SUBJECT' permission. This action will directly mitigate the risk of unauthorized entities specifying fraudulent subject names in certificates.

Steps to reproduce

1. Leverage a tool such as Certipy or WinPEAS to audit the available templates for dangerous permissions.

```
[?] +++++ Checking Template 'Tanium' +++++
[!] Template 'Tanium' has Flag 'ENROLLEE_SUPPLIES_SUBJECT'
[+] Identity 'KKMS\Domain Computers' has enrollment rights for template 'Tanium'
[!] Identity 'Local System' has 'GenericAll' permissions on template 'Tanium'
Template Name                           Tanium
Template distinguishedname:             CN=Tanium,CN=Certificate Templates,CN=Public Key Services,CN=Services,CN=Configu
ration,DC=corp,DC=kkms,DC=local
Date of Creation:                       01/09/2024 08:10:56
[+] Extended Key Usage:                 Client Authentication, Server Authentication
EnrollmentFlag:                         0
[!] CertificateNameFlag:                ENROLLEE_SUPPLIES_SUBJECT
[!] Template Permissions:               Local System : GenericAll
[+] Enrollment allowed for:             KKMS\Domain Computers
```

Dangerous permissions on Tanium

```
[?] +++++ Checking Template 'WorkstationAuthentication' +++++
[!] Template 'WorkstationAuthentication' has Flag 'ENROLLEE_SUPPLIES_SUBJECT'
[+] Identity 'KKMS\Domain Computers' has enrollment rights for template 'WorkstationAuthentication'
[!] Identity 'Local System' has 'GenericAll' permissions on template 'WorkstationAuthentication'
Template Name                           WorkstationAuthentication
Template distinguishedname:             CN=WorkstationAuthentication,CN=Certificate Templates,CN=Public Key Services,CN=
Services,CN=Configuration,DC=corp,DC=kkms,DC=local
Date of Creation:                       01/09/2024 08:10:55
[+] Extended Key Usage:                 Client Authentication
EnrollmentFlag:                         0
[!] CertificateNameFlag:                ENROLLEE_SUPPLIES_SUBJECT
[!] Template Permissions:               Local System : GenericAll
[+] Enrollment allowed for:             KKMS\Domain Computers
```

Dangerous permissions on WorkstationAuthentication

Reference(s):

- https://posts.specterops.io/certified-pre-owned-d95910965cd2
- https://www.blackhillsinfosec.com/abusing-active-directory-certificate-services-part-one/

RAKMS-015 Kerberoastable User Account

A user who is "kerberoastable" is someone with specific attributes that make them susceptible to a Kerberoasting attack. This vulnerability often arises due to Service Principal Names (SPNs) configured with a weak password in a Windows Active Directory environment. SPNs are associated with various services and are used for mutual authentication between a client and a service, such as SQL servers, web applications, or other resources.

While this vulnerability requires authentication, by leveraging RAKMS-001 and RAKMS-019 this requirement can be bypassed.

Affected systems

Zone	Hostname	IP
Corporate	SkyControl01	10.0.0.5

Vulnerability Scoring

Risk Assessment		CVSS v4.0 Score
Exploit Likelihood	Likely	7.1 High
Business Impact	Moderate	
Remediation Difficulty	Easy	
CVSS v4.0 Vector	CVSS:4.0/AV:N/AC:L/AT:N/PR:L/UI:N/VC:N/VI:H/VA:N/SC:N/SI:N/SA:N	

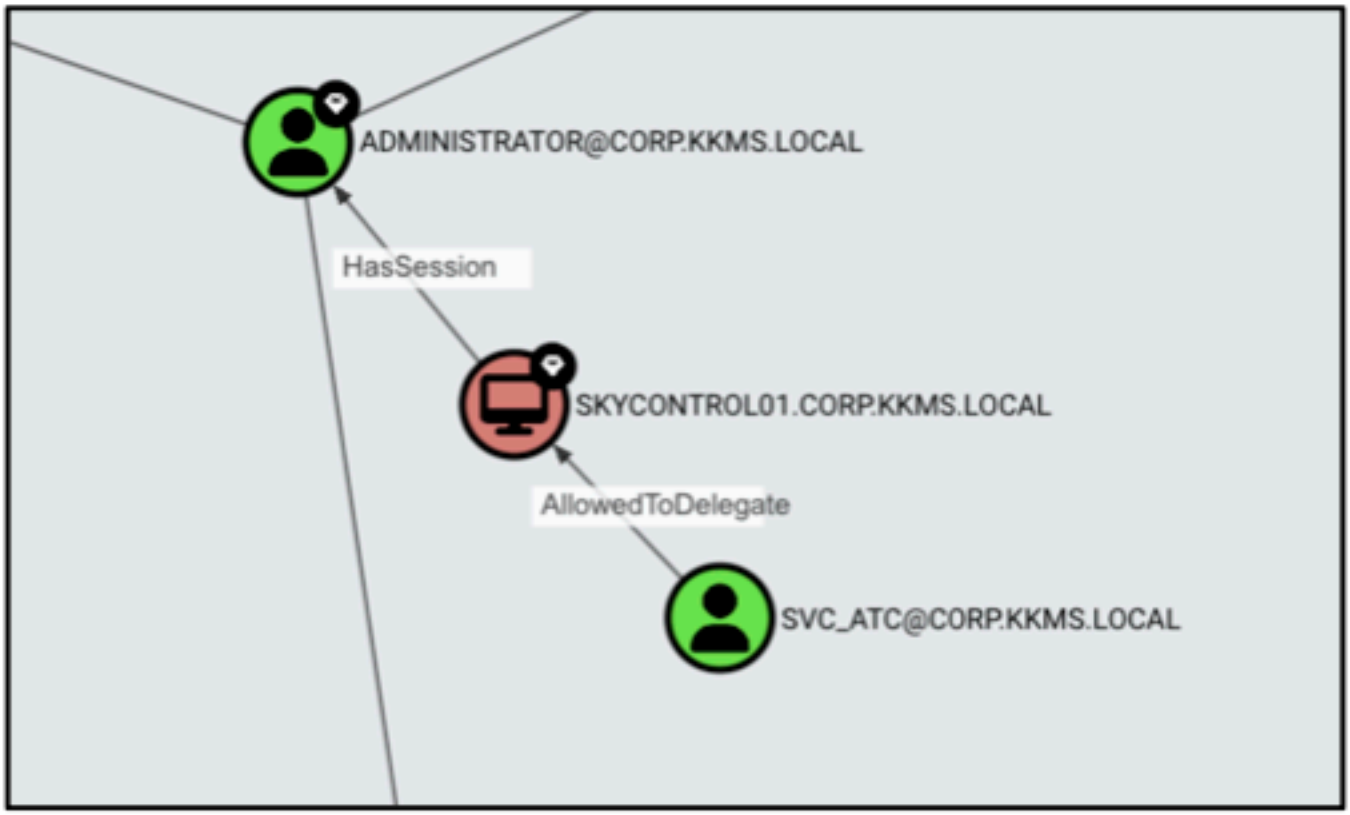
Technical Impact

In a Kerberoasting scenario, when an SPN is configured without adequate protection, an attacker can request the encrypted Ticket Granting Service (TGS) tickets associated with that SPN. They can then attempt to crack these tickets offline using various password-cracking tools and techniques, potentially compromising the user's credentials and gaining unauthorized access.

The impact of this is heightened by the constrained delegation rights of this account. Permitting it to impersonate users authenticated to file shares on the domain controller.

```
1670    [?] +++++ Searching for User with Constrained Delegation Rights +++++
1671    [!] Found constrained delegation rights for User 'svc_ATC':
1672    sAMAccountName:                         svc_ATC
1673    distinguishedName:                      CN=svc_ATC,CN=Users,DC=corp,DC=kkms,DC=local
1674    objectSid:                              S-1-5-21-3543778520-4226560126-3158920036-1279
1675    memberOf:                               CN=all,CN=Users,DC=corp,DC=kkms,DC=local
1676    [+] description:                        ATC Service Account
1677    [+] msDS-AllowedToDelegateTo:           cifs/SkyControl01
1678    pwdLastSet:                             01/09/2024 03:18:49
1679    userAccountControl:                     NORMAL_ACCOUNT, TRUSTED_TO_AUTH_FOR_DELEGATION
```

Output from WinPEAS showing delegation rights



Ability to leverage this permission to gain administrative rights

Business and Compliance Impact

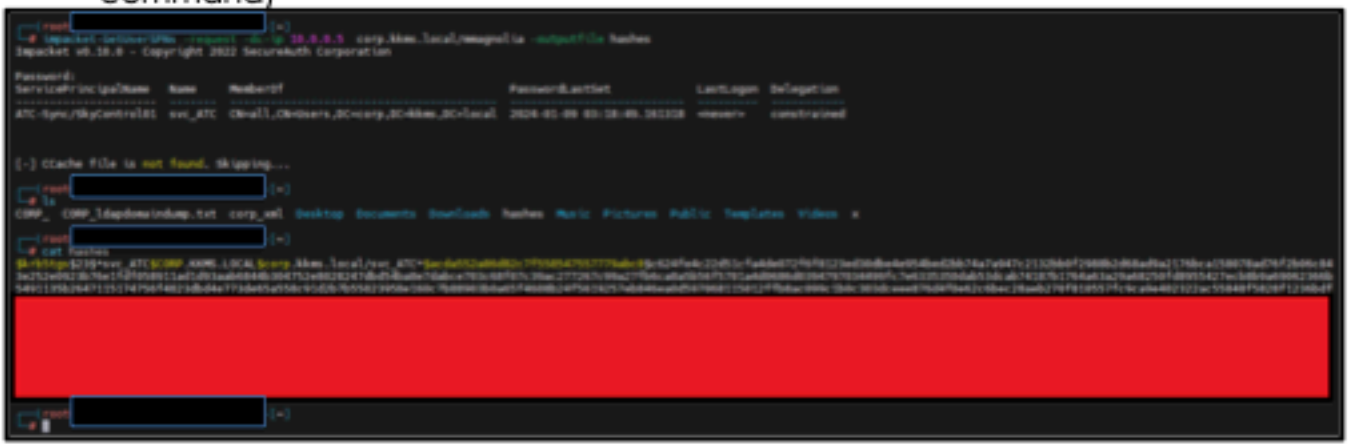
The presence of Kerberoastable user accounts poses a significant security risk for a business. Kerberoasting is an attack technique where attackers target weak or vulnerable accounts to extract password hashes, which can be cracked offline. This can lead to unauthorized access, data breaches, and the compromise of critical systems and sensitive data, resulting in financial losses and damage to an organization's reputation. It may also put the organization at risk of non-compliance with data protection regulations, potentially leading to legal consequences and fines. To mitigate these risks, businesses should identify and secure potentially Kerberoastable accounts through strong password policies and regular security assessments.

Remediation

We recommend all SPNs be configured with secure and complex passwords and that service account passwords be rotated regularly.

Steps to Reproduce

1. By leveraging a tool like Impacket's GetUserSPNs and a valid domain user, you are able to pull the hash from the svc_ATC account. (see screenshot for command)



Impacket pulling password hash (password hashes censored)

2. Using a tool like hashcat, because of the weak password on this account, we can crack the hash.

Hashcat cracking the weak password (hashes and cracked password censored)

Reference(s):

- https://www.netwrix.com/cracking_kerberos_tgs_tickets_using_kerberoasting.html

Medium Findings

RAKMS-016 Train API Unauthorized Train Registration

In the train network, three API endpoints are accessible that allow an attacker to arbitrarily add train objects to the train system without any authentication.

Affected systems

Zone	Hostnames	IPs
Train	Tram1 Tram2 Tram3	10.0.20.101 10.0.20.102 10.0.20.103

Vulnerability Scoring

Risk Assessment		CVSS v4.0 Score
Exploit Likelihood	Likely	6.9 Medium
Business Impact	Moderate	
Remediation Difficulty	Easy	
CVSS v4.0 Vector	CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:N/VI:L/VA:N/SC:N/SI:N/SA:N	

Technical Impact

This heavily impacts the integrity of the train network, as the train system can be flooded with fake trains.

Business and Compliance Impact

This impacts the RAKMS' ability to transport people throughout the Airport and fails to adhere to TSA guidelines on proper access controls of operational technology.

Remediation

While moving the train API to the train network is a great step in the right direction, we recommend adding proper authentication methods to restrict access to the API.

Steps to reproduce

Send a post request to http://10.0.20.101:8088/register with the correct data (see attached screenshot)

Train successfully registered using the /register train API

Reference(s):

- https://owasp.org/Top10/A01_2021-Broken_Access_Control/

RAKMS-017 Exposed Debug Endpoint On Debug Server

On the baggage check website, there is an exposed API endpoint that leaks debug information about the baggage claim system, allowing anyone to see confidential information.

Affected systems

Zone	Hostnames	IPs
Corporate	baggagecheckin.corp.kkms.local	10.0.0.33

Vulnerability Scoring

Risk Assessment		CVSS v4.0 Score
Exploit Likelihood	Likely	6.9 Medium
Business Impact	Moderate	
Remediation Difficulty	Easy	
CVSS v4.0 Vector	CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:L/VI:N/VA:N/SC:N/SI:N/SA:N	

Technical Impact

This exposes an informational endpoint that

Business and Compliance Impact

Remediation

Steps to reproduce

Go to baggagecheckin.corp.kkms.local/kiosk/go/debug or 10.0.0.33/kiosk/go/debug

Train successfully registered using the /register train API

Reference(s):

- https://owasp.org/Top10/A01_2021-Broken_Access_Control/

RAKMS-018 Anonymous Bind Enabled on LDAP

Any users on the network without authentication are able to query the domain controller for a list of users in the environment.

Affected systems

Zone	Hostnames	IPs
Corporate	SKYCONTROL01	10.0.0.5

Vulnerability Scoring

Risk Assessment		CVSS v4.0 Score
Exploit Likelihood	Likely	6.9 Medium
Business Impact	Moderate	
Remediation Difficulty	Easy	
CVSS v4.0 Vector	CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:L/VI:N/VA:N/SC:N/SI:N/SA:N	

Technical Impact

By leveraging this vulnerability, a threat actor would be able to enumerate valid usernames in the environment to then leverage in further attacks.

Business and Compliance Impact

User enumeration via anonymous LDAP bind poses significant business risks. It allows attackers to identify valid user accounts within an organization's directory, leading to targeted phishing and social engineering attacks. This can result in data breaches, financial losses, and damage to an organization's reputation. Non-compliance with data protection regulations and the diversion of resources for incident response are additional adverse effects, making it essential for businesses to implement robust security measures to prevent user enumeration.

Remediation

We recommend permissions around LDAP binds be hardened to prevent anonymous binds from giving information.

Steps to reproduce

Reference(s):

- https://owasp.org/Top10/A01_2021-Broken_Access_Control/

RAKMS-019 ASREPRoastable User

The ASREPRoast attack looks for users without pre-authentication required. This means that anyone on the network can request the Domain Controller on behalf of those users, requesting a message that contains the password hash of that user. This hash can then be cracked offline.

Affected systems

Zone	Hostnames	IPs
Corporate	SKYCONTROL01	10.0.0.5

Vulnerability Scoring

Risk Assessment		CVSS v4.0 Score
Exploit Likelihood	Likely	6.9 Medium
Business Impact	Moderate	
Remediation Difficulty	Easy	
CVSS v4.0 Vector	CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:N/VI:L/VA:N/SC:N/SI:N/SA:N	

Technical Impact

This allows an unauthenticated user to gain a foothold in the network if the password is successfully cracked.

Business and Compliance Impact

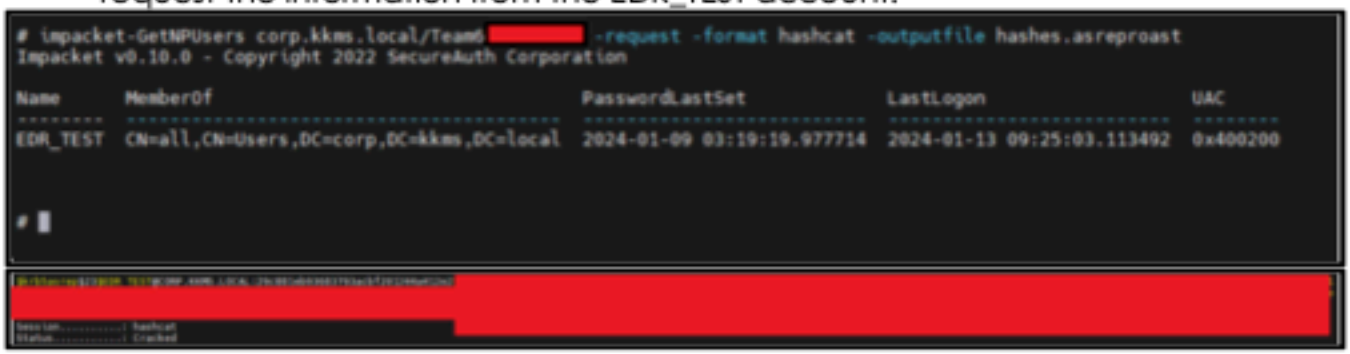
The presence of ASREPRoastable user accounts poses a significant security risk for a business. This allows anyone on the network to compromise the systems in the network, which can lead to unauthorized access, data breaches, and the compromise of critical systems, and the compromise of critical systems and sensitive data, resulting in financial losses and damage to an organization's reputation. It may also put the organization at risk of non-compliance with data protection regulations, potentially leading to legal consequences and fines. To mitigate these risks, businesses should identify and secure potentially ASREPRoast-able accounts through strong password policies and regular security

Remediation

We recommend you require Kerberos pre-authentication on the EDR_TEST account. See the source below for more information on the remediation info.

Steps to reproduce

1. Using a tool like Impacket's GetNPUsers, an unauthenticated user can request the information from the EDR_TEST account.



Though authenticated, shown above is an example of retrieval of the user's password hash.

Reference(s):

- https://tcm-sec.com/pre-authentication-in-ad-environments/
- https://www.tenable.com/blog/how-to-stop-the-kerberos-pre-authentication-attack-in-active-directory

RAKMS-020 Unauthenticated Equipment Requisition System

A public endpoint allows for anonymous users on the internet to create purchase orders for tools, without authentication.

Affected systems

Zone	Endpoint
AWS	http://rakmstoolrequisition20240111034801124200000007.s3-website-us-east-1.amazonaws.com/

Vulnerability Scoring

Risk Assessment		CVSS v4.0 Score
Exploit Likelihood	Possible	6.9 Medium
Business Impact	Severe	
Remediation Difficulty	Medium	
CVSS v4.0 Vector	CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:N/VI:L/VA:L/SC:N/SI:N/SA:N	

Technical Impact

This vulnerability would allow anyone in the world to purchase tools at the company's expense, resulting in undefined losses to company revenue.

Business and Compliance Impact

Unforeseen costs could arise, destroying created budgets. This could cause financial ruin in the worst-case scenario, where this is abused considerably. The company would take a massive hit to its reputation by allowing unauthorized purchases like this.

Remediation:

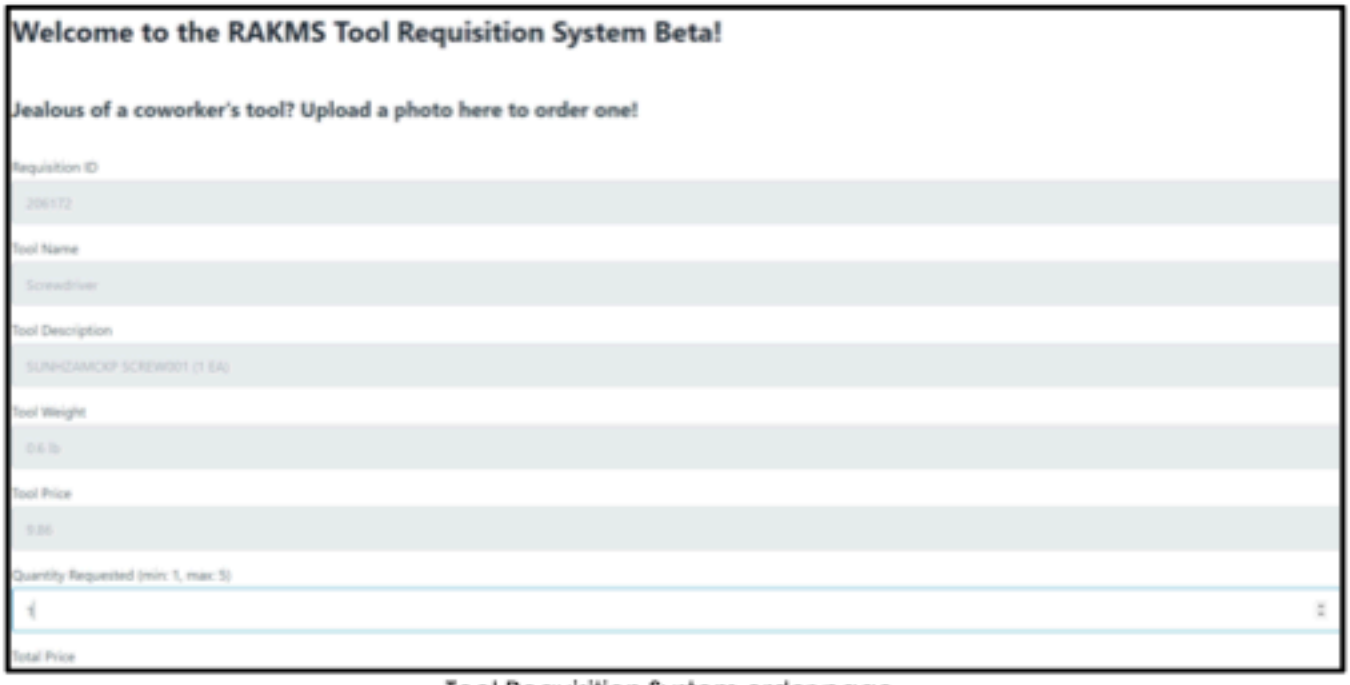
We recommend adding a login to the order portal and hosting the application locally to reduce the attack surface.

Steps to reproduce

First go to the endpoint, upload an image of the tool you want to order, then hit 'Submit Query'.

Tool Requisition System main page

Then you'll be taken to a form to verify your order, set the quantity, and submit your order.



Tool Requisition System order page

Reference(s):

- https://cwe.mitre.org/data/definitions/862.html

RAKMS-021 Train Dashboard Vulnerable to DOS

The train dashboard showing status on all of the trains (http://10.0.20.100:3000/home) is very susceptible to DOS attacks. This vulnerability could allow an attacker to temporarily deny legitimate access to the dashboard by flooding the service with malicious requests.

Affected systems

Zone	Hostname	IP
Train	tram-ops	10.0.20.100

Vulnerability Scoring

Risk Assessment		CVSS v4.0 Score
Exploit Likelihood	Possible	6.9 Medium
Business Impact	Moderate	
Remediation Difficulty	Medium	
CVSS v4.0 Vector	CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:N/VI:N/VA:L/SC:N/SI:N/SA:N	

Technical Impact

This can temporarily impact the train information displays, causing slowdowns.

Business and Compliance Impact

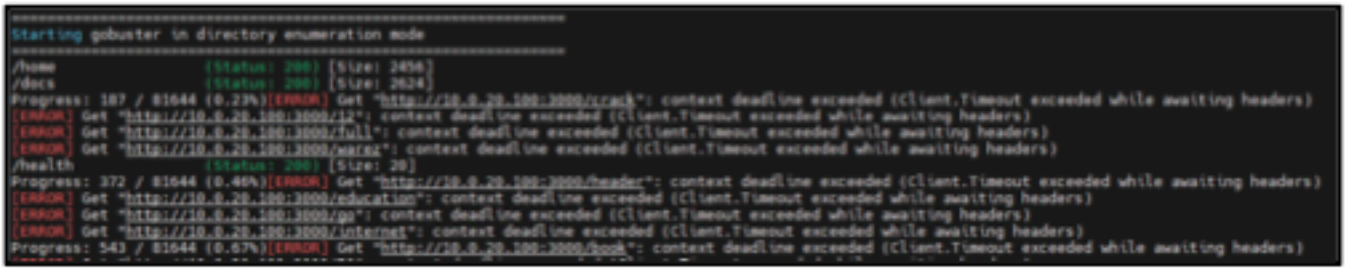
This impacts the RAKMS' ability to monitor the trains and transport people throughout the Airport.

Remediation

We recommend adding an ACL rule to block IP addresses that send too much data within a particular timeframe, as this would prevent a single host from overloading the system.

Steps to reproduce

1. Use a directory enumeration tool to send multiple requests in rapid succession.



Gobuster causing the train dashboard to timeout and slow down

Reference(s):

- https://github.com/OJ/gobuster

RAKMS-022 No TLS or Self-Signed Certificates on Webapps

Unencrypted web apps and APIs allow an attacker to perform man-in-the-middle attacks by spoofing services, as well as allowing an attacker to view sensitive data or credentials over the network. Untrusted web apps with Self-Signed certificates will error out on web browsers, which will negatively impact a customer's ability to interact with RAKMS services.

Affected systems

Zone	Hostname	IP
Corporate, Guest, Train	SkyController01, CESSNA-EXCHANGE, BAGGAGECLAIM, EmployeeTime-DB Login, Flight Dashboard, TSA, RAKMS-Guest-Wifi, Tram-Ops, Tram1, Tram2, Tram3	10.0.0.5, 10.0.0.6, 10.0.0.33, 10.0.0.43, 10.0.0.100, 10.0.200.5, 10.0.200.43, 10.0.200.100, 10.0.20.101, 10.0.20.102, 10.0.20.103

Vulnerability Scoring

Risk Assessment		CVSS v4 Score
Exploit Likelihood	Possible	6.3 Medium
Business Impact	Mild	
Remediation Difficulty	Medium	
CVSS v4 Vector	AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:L/A:N	

Technical Impact

An attacker could use wireshark or another packet capturing tool to sniff credentials or sensitive data from the vulnerable endpoints. Additionally, an attacker could create a malicious endpoint and perform a man-in-the-middle attack, allowing the attacker to capture and manipulate the data in transit.

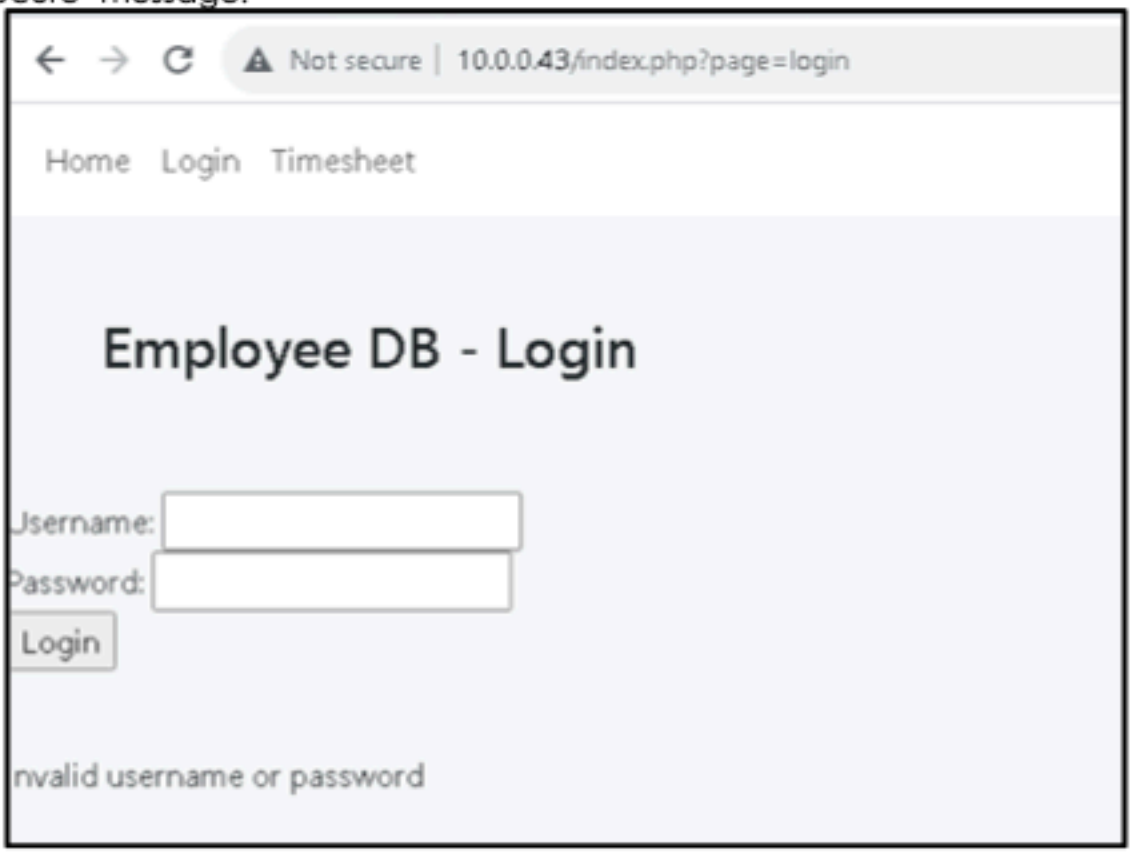
Business and Compliance Impact

Transferring sensitive customer and business data without encryption is a major liability. Depending on the data being transferred, unencrypted endpoints can be a direct compliance violation of the PCI DSS. Although a Self-Signed certificate

encrypts traffic, it creates friction in the customer experience, which will negatively impact the business as a whole.

Remediation
We recommend adding TLS encryption to every single web page hosted in the environment. This should also go through a certificate authority within the domain, so they are all encrypted and trusted within the domain. Overall, this will significantly improve the security posture of the environment.

Steps to Reproduce
Go to one of the insecure endpoints in a browser and look at the http protocol or the 'Not secure' message.



Login portal showing as 'Not secure'

Reference(s):
- https://cwe.mitre.org/data/definitions/319.html
- https://https.cio.gov/faq/
- https://listings.pcisecuritystandards.org/documents/PCI_DSS-QRG-v3_2_1.pdf

RAKMS-023 Cross-Service Confused Deputy

Multiple roles within the AWS account are vulnerable to a Cross-Service Confused Deputy attack, allowing any user with credentials to assume a role with higher privileges for a service. Through this, an attacker could obtain additional network access and potentially compromise additional RAKMS systems.

Affected systems

Zone
AWS

Vulnerability Scoring

Risk Assessment		CVSS v4.0 Score
Exploit Likelihood	Possible	6.1 Medium
Business Impact	Moderate	
Remediation Difficulty	Easy	
CVSS v4.0 Vector	CVSS:4.0/AV:N/AC:L/AT:P/PR:L/UI:N/VC:H/VI:L/VA:L/SC:N/SI:N/SA:N	

Technical Impact

Unauthorized access due to a Cross-Service Confused Deputy attack poses a significant risk for RAKMS. The finding could lead to the exposure of sensitive information, confidential data, and intellectual property, depending on the service that becomes available. This unauthorized access may result in data manipulation, compromising the integrity of stored information. The attacker could also escalate privileges, gaining access to critical resources and potentially disrupting services, leading to downtime for legitimate users.

Business and Compliance Impact

Unauthorized access can lead to exposure of sensitive data, and data manipulation, significantly impacting the trust of RAKMS customers and the integrity of company data.

Remediation

We recommend limiting access for assuming roles that allow access to a principal service to specific role ARNs or account IDs within the role policy. Use the

aws:SourceArn and aws:SourceAccount global condition context keys in trust relationship policies to limit the permissions that a service has to a specific resource.

Steps to reproduce

- aws iam get-account-authorization-details
- search for roles that allow assuming the role with a service


```
{
    "Path": "/",
    "RoleName": "lambda-barcode-role",
    "RoleId": "AROAZ3MTAMYRJNKGQUILE",
    "Arn": "arn:aws:iam::677302527522:role/lambda-barcode-role",
    "CreateDate": "2024-01-11T03:48:01Z",
    "AssumeRolePolicyDocument": {
        "Version": "2012-10-17",
        "Statement": [
            {
                "Sid": "",
                "Effect": "Allow",
                "Principal": {
                    "Service": "lambda.amazonaws.com"
                },
                "Action": "sts:AssumeRole"
            }
        ]
    },
    "InstanceProfileList": [],
    "RolePolicyList": [],
    "AttachedManagedPolicies": [
        {
            "PolicyName": "lambda-barcode-policy",
            "PolicyArn": "arn:aws:iam::677302527522:policy/lambda-barcode-policy"
        }
```


Account details showing "sts:AssumeRole" and Service: XXX.amazonaws.com

Reference(s):

- https://docs.aws.amazon.com/iotevents/latest/developerguide/cross-service-confused-deputy-prevention.html
- https://medium.com/cloud-security/confused-deputy-attack-in-iam-resource-and-assumerole-policies-8fea3e2553b2

RAKMS-024 Insecure Role Privileges in AWS

Several roles in AWS allow any user to assume their privileges, through which the user could view encrypted strings, including passwords, in plaintext. This could allow for an attacker to assume a privileged role and gain further access, potentially reusing passwords in other RAKMS systems.

Affected systems

Zone	Roles
AWS	dev-barcode-role dev-lambda-bar-role dev-lambda-role dev-s3-role dev1-role dev2-lambda-role dev2-role secrets-viewer secret-viewer

Vulnerability Scoring

Risk Assessment		CVSS v4.0 Score
Exploit Likelihood	Likely	6.0 Medium
Business Impact	Moderate	
Remediation Difficulty	Moderate	
CVSS v4.0 Vector	CVSS:4.0/AV:N/AC:L/AT:P/PR:L/UI:N/VC:H/VI:L/VA:N/SC:N/SI:N/SA:N	

Technical Impact

Allowing any IAM identity to assume these roles allows any user under the AWS account to escalate or gain new privileges, such as being able to view SSM secret strings. These often include passwords, API keys, and other sensitive information, causing a loss of confidentiality and potentially providing a method to escalate privileges further.

Business and Compliance Impact

Due to the privilege escalation abilities granted to users in AWS, employees and attackers alike could potentially disrupt AWS related business operations. An attacker could open RAKMS to potential compliance fines and regulation.

Remediation:
We strongly recommend limiting the ability to assume roles to only the identities that need access to those roles by ARN.

Steps to reproduce

- aws iam get-account-authorization-details
- search for roles that allows the action sts:AssumeRole for the principal AWS: *
- aws sts assume-role –arn $ROLE_ARN

```
Pacu (no:imported-default) > assume_role arn:aws:iam::677302527522:role/dev-barco
de-role
AWS key is now no/arn:aws:sts::677302527522:assumed-role/dev-barcode-role/assume-
role.
Pacu (no:no/arn:aws:sts::677302527522:assumed-role/dev-barcode-role/assume-role)
> aws s3 ls

An error occurred (AccessDenied) when calling the ListBuckets operation: Access D
enied

Pacu (no:no/arn:aws:sts::677302527522:assumed-role/dev-barcode-role/assume-role)
> aws s3api list-buckets

An error occurred (AccessDenied) when calling the ListBuckets operation: Access D
enied

Pacu (no:no/arn:aws:sts::677302527522:assumed-role/dev-barcode-role/assume-role)
> aws s3 ls s3://rakmsbarcode20240111034800721800000004
2024-01-12 11:32:14      16339 0112163210.svg
2024-01-12 11:33:07      16339 0112163304.svg
2024-01-12 11:44:22      11797 0112164419.svg
2024-01-12 11:47:27      31812 0112164725.svg
2024-01-12 11:47:42      11541 0112164740.svg
2024-01-12 11:47:45      28233 0112164743.svg
2024-01-12 11:47:48      11587 0112164746.svg
2024-01-12 11:47:52      11413 0112164750.svg
2024-01-12 11:48:00      32340 0112164758.svg
2024-01-12 11:48:02      11847 0112164801.svg
2024-01-12 11:48:07      11537 0112164805.svg
2024-01-12 11:48:13      11758 0112164811.svg
2024-01-12 11:51:23      33302 0112165121.svg
2024-01-12 11:53:32      27703 0112165331.svg
2024-01-12 11:54:40      27703 0112165439.svg
2024-01-12 11:54:50      24307 0112165448.svg
2024-01-12 11:57:36      27445 0112165735.svg
2024-01-12 11:57:47      27445 0112165745.svg
2024-01-12 11:57:51      27445 0112165750.svg
```

Assuming the dev-barcode-role and using the gained permissions to list the contents of a bucket

```
        {
            "Path": "/",
            "RoleName": "secret_viewer",
            "RoleId": "AROAZ3MTAMYRIIFPQ5QPC",
            "Arn": "arn:aws:iam::677302527522:role/secret_viewer",
            "CreateDate": "2024-01-11T03:48:08Z",
            "AssumeRolePolicyDocument": {
                "Version": "2012-10-17",
                "Statement": [
                    {
                        "Effect": "Allow",
                        "Principal": {
                            "AWS": "*"
                        },
                        "Action": "sts:AssumeRole"
                    },
                    {
                        "Effect": "Deny",
                        "Principal": {
                            "AWS": "*"
                        },
                        "Action": "sts:AssumeRole",
                        "Condition": {
                            "ArnNotEquals": {
                                "aws:PrincipalArn":
"arn:aws:iam::677302527522:user/*"
                            }
                        }
                    }
                ]
            },
```

Insecure permissions assigned to secret_viewer role, allowing any user to assume

Reference(s):

- https://docs.aws.amazon.com/IAM/latest/UserGuide/best-practices.html?ref=wellarchitected#grant-least-privilege

RAKMS-025 SMB Signing Not Required

SMB signing is not required, which means that data transferred over the Server Message Block protocol is not digitally signed for authentication and integrity. This absence of SMB signing can expose the network to security risks, as it allows for potential data tampering and unauthorized access.

Affected systems

Zone	Domain
Corporate	corp.kkms.local

Vulnerability Scoring

Risk Assessment		CVSS v4.0 Score
Exploit Likelihood	Possible	5.6 Medium
Business Impact	Moderate	
Remediation Difficulty	Easy	
CVSS v4.0 Vector	CVSS:4.0/AV:N/AC:L/AT:N/PR:L/UI:N/VC:N/VI:N/VA:N/SC:L/SI:L/SA:L	

Technical Impact

Without this critical authentication and data integrity measure, the network becomes susceptible to man-in-the-middle attacks, where malicious actors can intercept and modify data as it traverses the SMB protocol.

Business and Compliance Impact

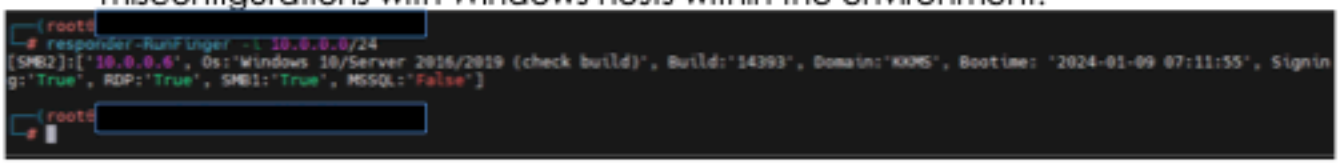
The absence of SMB (Server Message Block) signing requirements can have serious business impacts. Without SMB signing, data transfer between devices in a network becomes vulnerable to interception and tampering, potentially leading to unauthorized access, data breaches, and security incidents. This can result in financial losses, damage to an organization's reputation, and legal consequences due to potential non-compliance with data protection regulations. Implementing SMB signing and other security measures is crucial for businesses to mitigate these risks and protect their network resources and sensitive data.

Remediation:

We recommend SMB signing be required on all Windows hosts within the network.

Steps to reproduce

1. By leveraging a tool such as responder-RunFinger you can enumerate misconfigurations with Windows hosts within the environment.



Runfinger showing an example of

RAKMS-026 Add-Computer Improper Permissions

Any user in the group 'Authorized Users' can add a computer to the domain. This allows attackers to add malicious devices to the domain, as well as use their own devices as an entry point for privilege escalation tactics.

Affected systems

Zone	Domain
Corporate	corp.kkms.local

Vulnerability Scoring

Risk Assessment		CVSS v4.0 Score
Exploit Likelihood	Possible	5.3 Medium
Business Impact	Moderate	
Remediation Difficulty	Easy	
CVSS v4.0 Vector	CVSS:4.0/AV:N/AC:L/AT:N/PR:L/UI:N/VC:N/VI:N/VA:N/SC:L/SI:L/SA:L	

Technical Impact

This attack in isolation has minimal impact on the environment as a whole, however, when combined with other exploits, can create an attack chain from no creds to domain admin.

Business and Compliance Impact

This attack in isolation has minimal impact on the environment as a whole, however, when combined with other exploits, can create an attack chain from no creds to domain admin.

Remediation:

We recommend changing the 'Add-Computer' role in the domain controller to only include domain admins.

Steps to reproduce

2. Run Winpeas on the domain controller to see the permissions. (see Tools Used Appendix for more info)

```
[?] +++++ Checking Add-Computer Permissions +++++
[+] Filtering found identities that can add a computer object to domain 'corp.kkms.local':
[!] The Machine Account Quota is currently set to 10
[!] Every member of group 'Authenticated Users' can add a computer to domain 'corp.kkms.local'

distinguishedName:                      CN=S-1-5-11,CN=ForeignSecurityPrincipals,DC=corp,DC=kkms,DC=local
objectSid:                              S-1-5-11
memberOf:                               CN=Pre-Windows 2000 Compatible Access,CN=Builtin,DC=corp,DC=kkms,DC=local
                                        CN=Certificate Service DCOM Access,CN=Builtin,DC=corp,DC=kkms,DC=local
                                        CN=Users,CN=Builtin,DC=corp,DC=kkms,DC=local
```

Winpeas output showing Add-Computer permission applied to 'Authenticated Users' group

Refrence(s)

- https://github.com/carlospolop/PEASS-ng/tree/master/winPEAS

RAKMS-027 Misconfigured Webroot Directory

Misconfigured Webroot Directory on a website, while not a critical vulnerability, allows users to view and download files. This could include sensitive data or confidential information which can potentially harm a company's reputation and raise security concerns. In this particular case it allowed for RAKMS-029

Affected systems

Zone	Hostname	IP
Corporate	AFWS	10.0.0.100

Vulnerability Scoring

Risk Assessment		CVSS v4.0 Score
Exploit Likelihood	Likely	5.1 Medium
Business Impact	Moderate	
Remediation Difficulty	Easy	
CVSS v4.0 Vector	CVSS:4.0/AV:L/AC:L/AT:N/PR:N/UI:N/VC:L/VI:N/VA:N/SC:L/SI:N/SA:N	

Technical Impact

If confidential information was available, an attacker could easily find the information and use it for other attacks. The current access could potentially allow an attacker (if they had the ability to upload files) to host a webshell on the server.

Business and Compliance Impact

Misconfigured Webroot Directories pose significant business and compliance risks. From a business perspective, it can lead to unauthorized access to sensitive files, potentially resulting in data breaches and reputational damage. In terms of compliance, it violates data protection regulations and security standards, potentially leading to legal consequences and regulatory non-compliance, making it essential for organizations to address and mitigate this vulnerability.

Remediation

We recommend avoiding passing user-supplied input to filesystem APIs whenever possible. Many functions can be rewritten to maintain their intended functionality in a

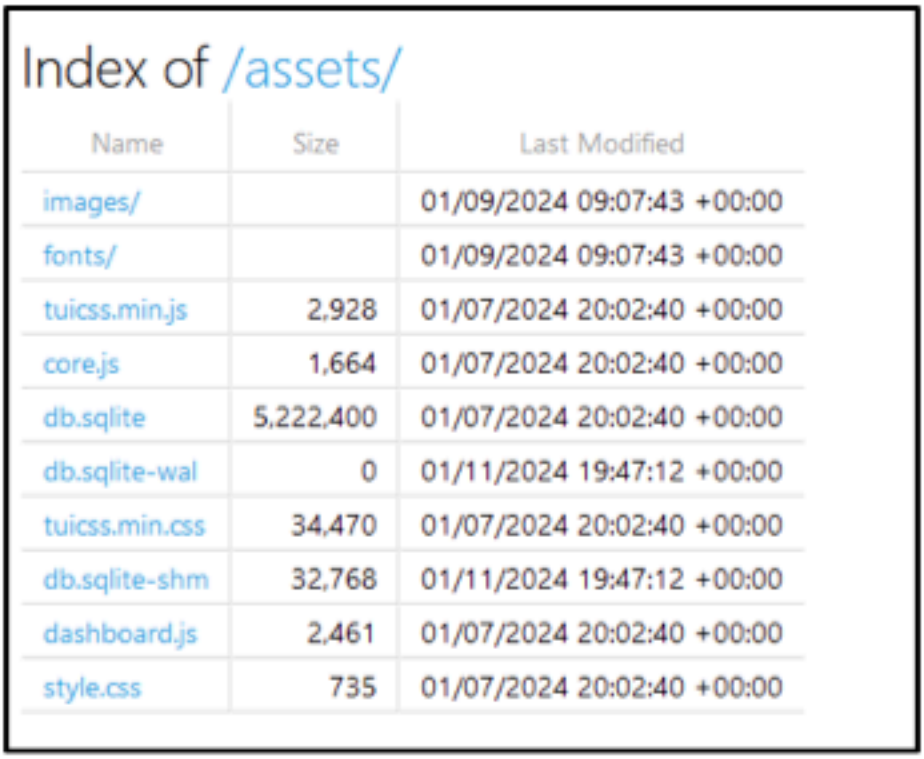
more secure manner. However, if necessary in order to use user-submitted content with filesystem APIs, implement two layers of defense.

First, validate the user-supplied input by comparing it to a whitelist of acceptable values or ensuring it contains only approved content.

Secondly, ensure that the canonicalized path starts with the expected base directory, verifying the correctness of the base directory at the beginning of the path. These precautions are crucial for maintaining security when working with user-generated input in filesystem operations.

Steps to Reproduce

1. Visit the site: http://10.0.0.100/assets/



Index of /assets/

Name	Size	Last Modified
images/		01/09/2024 09:07:43 +00:00
fonts/		01/09/2024 09:07:43 +00:00
tuicss.min.js	2,928	01/07/2024 20:02:40 +00:00
core.js	1,664	01/07/2024 20:02:40 +00:00
db.sqlite	5,222,400	01/07/2024 20:02:40 +00:00
db.sqlite-wal	0	01/11/2024 19:47:12 +00:00
tuicss.min.css	34,470	01/07/2024 20:02:40 +00:00
db.sqlite-shm	32,768	01/11/2024 19:47:12 +00:00
dashboard.js	2,461	01/07/2024 20:02:40 +00:00
style.css	735	01/07/2024 20:02:40 +00:00

Exposed files accessible through browser

Reference(s):

https://vulncat.fortify.com/en/detail?id=desc.dynamic.xtended_preview.web_server_misconfiguration_directory_listing

RAKMS-028 Hard-Coded Credentials

In the corporate network, due to RAKMS-028, an attacker can access a file containing hard-coded credentials within a javascript program. This could lead to an attacker gaining access to the service using these credentials, creating an overarching attack chain against the AFWS machine and service.

Affected systems

Zone	Hostnames	IPs
Corp	AFWS	10.0.20.100

Vulnerability Scoring

Risk Assessment		CVSS v4.0 Score
Exploit Likelihood	Likely	5.1 Medium
Business Impact	Moderate	
Remediation Difficulty	Easy	
CVSS v4.0 Vector	CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:L/VI:N/VA:N/SC:N/SI:N/SA:N	

Technical Impact

The hard-coded credential could lead to a broader attack chain towards the AFWS machine, or potentially other endpoints. An attacker could reverse the javascript code alongside the credentials to enumerate the database.

Business and Compliance Impact

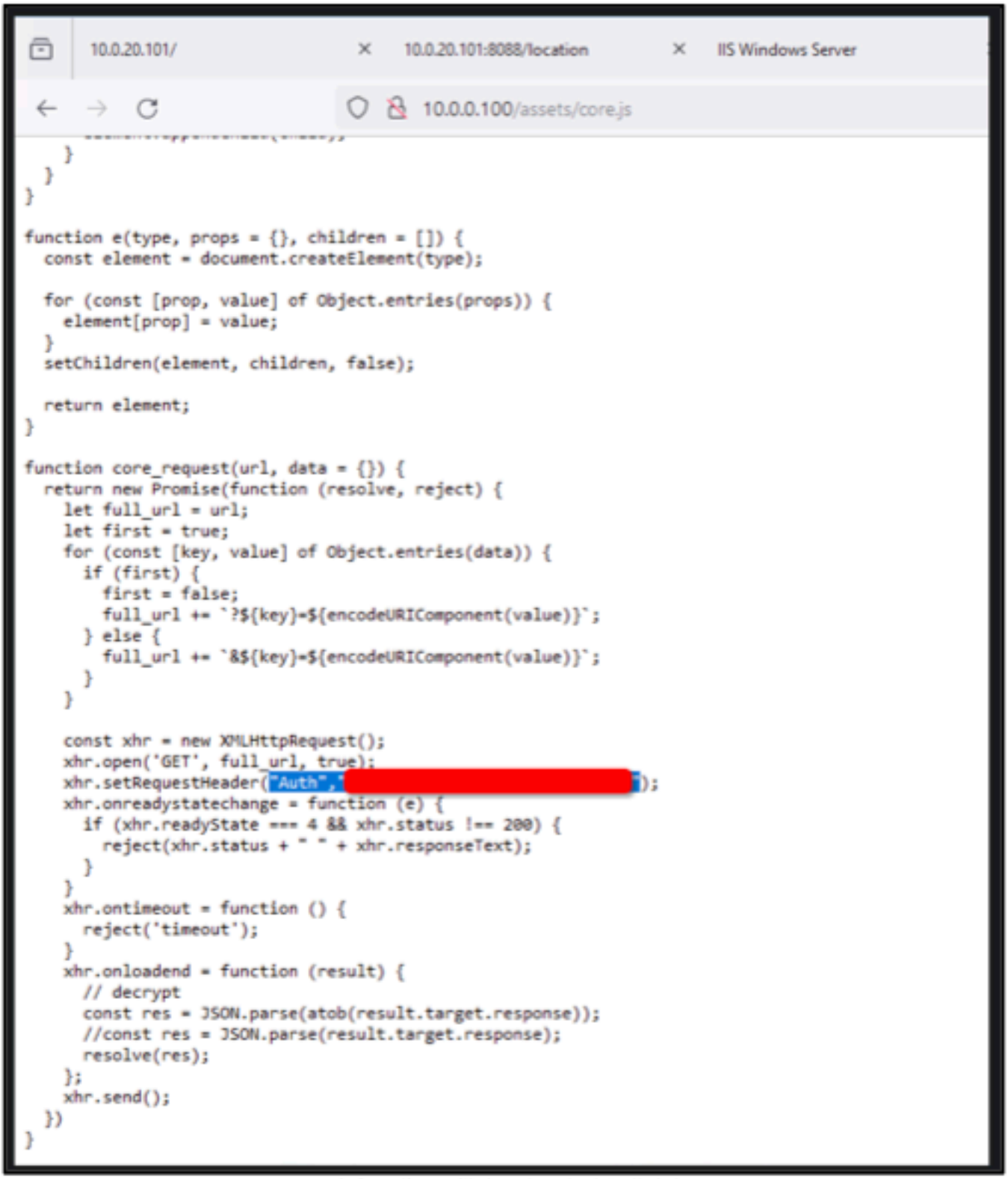
This finding could lead to a significant impact on the RAKMS Flight Dashboard, rendering it incorrect, malicious, or unavailable. The resulting impact could lead to a breach of privacy if the attacker utilized the credentials to access to database. If the credentials allow for the manipulation of database records, it could potentially affect integrity.

Remediation

While moving the train API to the train network is a great step in the right direction, we recommend adding proper authentication methods to restrict access to the API.

Steps to reproduce

Navigate to: http://10.0.0.100/assets/core.js (see attached screenshot)



core.js function with hardcoded Auth token

Reference(s):

https://owasp.org/www-community/vulnerabilities/Use_of_hard-coded_password

RAKMS-029 SMBv1 Enabled

SMBv1, a legacy and outdated version of the Server Message Block protocol, is enabled on the target SMB servers. This poses a significant security risk, as SMBv1 is known to have numerous vulnerabilities and has been widely exploited by malicious actors.

Affected systems

Zone	Hostname	IP
Corporate	CESSNA-EXCHANGE	10.0.0.6

Vulnerability Scoring

Risk Assessment		CVSS v4 Score
Exploit Likelihood	Possible	5.1 Medium
Business Impact	Moderate	
Remediation Difficulty	Easy	
CVSS v4 Vector	CVSS:4.0/AV:L/AC:L/AT:N/PR:N/UI:N/VC:L/VI:N/VA:N/SC:N/SI:N/SA:N	

Technical Impact

Enabling SMBv1 opens the door to a wide array of potential threats, such as remote code execution, man-in-the-middle attacks, and data breaches. Attackers can exploit these vulnerabilities to gain unauthorized access to sensitive company data, compromise network integrity, and potentially disrupt business operations.

Business and Compliance Impact

Enabling SMBv1 (Server Message Block version 1) in a network can have significant business impacts. SMBv1 is an outdated and insecure protocol that can expose an organization to security risks. It is vulnerable to various types of attacks, such as WannaCry and NotPetya ransomware, which can lead to data breaches, operational disruptions, and financial losses. Moreover, continued use of SMBv1 may result in compliance violations with data protection regulations, potential legal consequences, and damage to an organization's reputation. To minimize these risks, businesses should disable SMBv1 and upgrade to more secure versions of the protocol.

Remediation
We recommend having SMBv1 disabled on all Windows hosts within the network.

Steps to Reproduce
By leveraging a tool such as responder-RunFinger you can enumerate misconfigurations with Windows hosts within the environment.

Command output of responder-RunFinger

Reference(s):
- https://learn.microsoft.com/en-us/windows-server/storage/file-server/troubleshoot/detect-enable-and-disable-smbv1-v2-v3?tabs=server

Low Findings

RAKMS-030 Missing "httpOnly" Cookie Attribute

The employee database is missing the 'httpOnly' attribute on the session cookie which allows it to be accessed by JavaScript which could lead to session hijacking attacks.

Affected systems

Zone	Hostname	IP
Corporate	Employee-DB Login	10.0.0.43

Vulnerability Scoring

Risk Assessment		CVSS v4 Score
Exploit Likelihood	Unlikely	1.0 Low
Business Impact	Moderate	
Remediation Difficulty	Easy	
CVSS v4.0 Vector	CVSS:4.0/AV:L/AC:H/AT:N/PR:L/UI:A/VC:L/VI:L/VA:N/SC:N/SI:N/SA:N	

Technical Impact

The missing 'httpOny' cookie attribute allows JavaScript access to cookies, creating a risk of session hijacking and unauthorized data access

Business and Compliance Impact

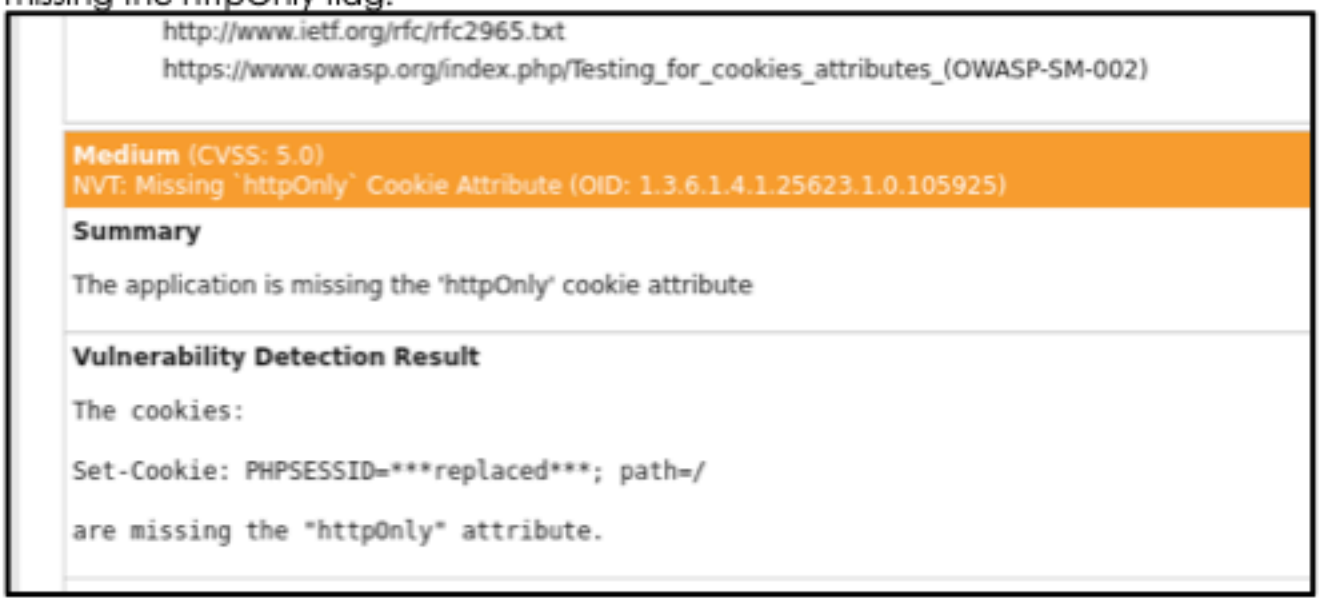
Missing the 'httpOnly' attribute alone does not directly violate compliance standards, but it does create a security risk that could potentially result in non-compliance if it leads to data breaches or unauthorized access to sensitive information.

Remediation

To remediate the vulnerability of the missing 'httpOnly' cookie attribute, implement the 'httpOnly' attribute for all cookies used in the application to prevent JavaScript access.

Steps to Reproduce

In developer tools, view the cookies of the website and ensure that none of them are missing the httpOnly flag.



OpenVAS scan showing httpOnly cookie attribute missing

Reference(s):

- https://www.rapid7.com/db/vulnerabilities/http-cookie-http-only-flag/

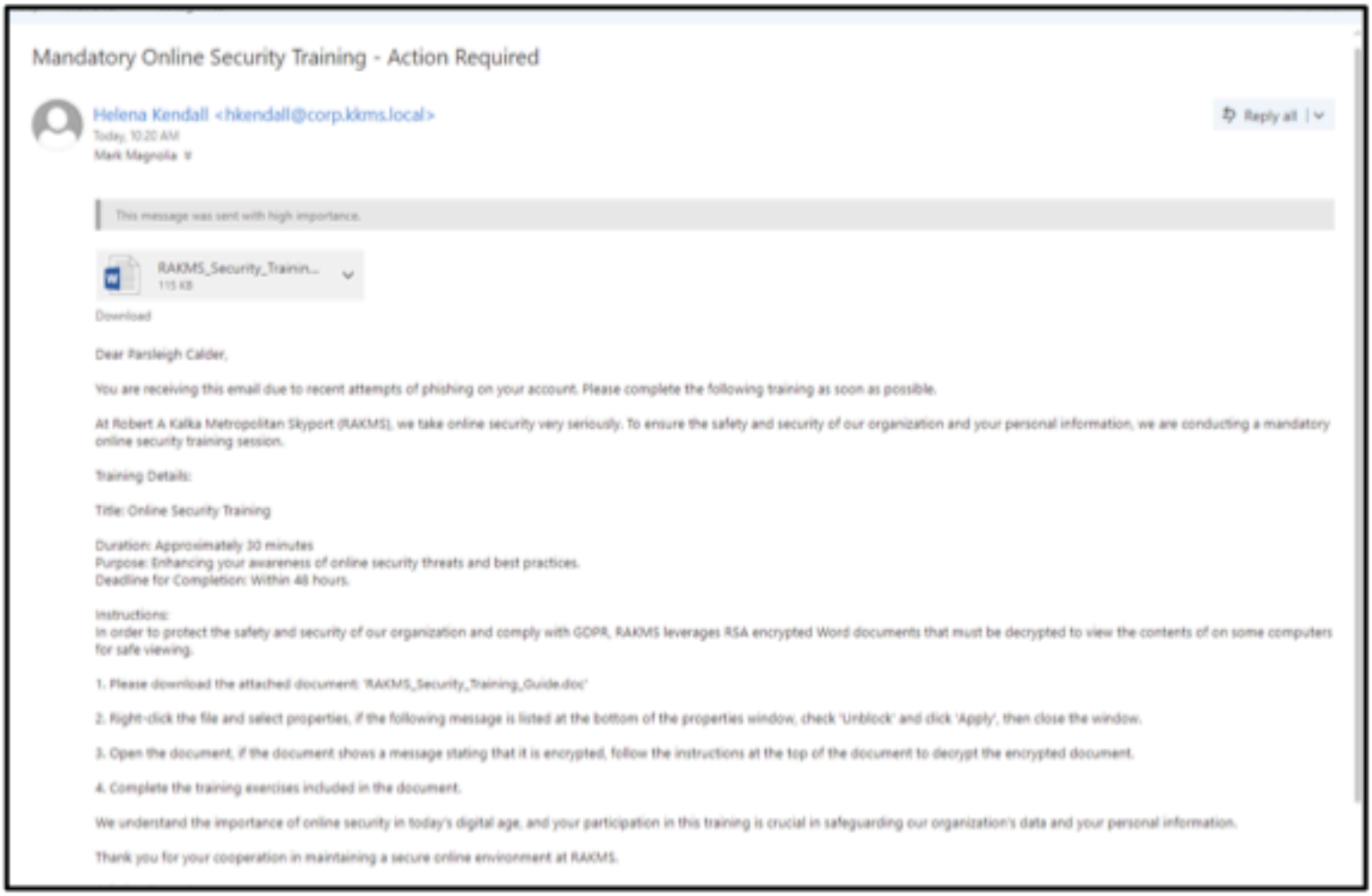
Appendix A - Phishing Engagement

Executive Summary

As part of its scheduled penetration test, RAKMS engaged Finals-XX to conduct a limited-scope and email phishing exercise against its employees. Hackers frequently use phishing emails to entice the recipient to click a malicious link, visit a fraudulent website, or launch a malicious program. This personal information for both Social Engineering attempts would include items such as a Social Security Number, user ID, and/or password. Some fraudulent websites may also be virus-laden and can be used to install malware on a workstation.

Phishing Email Pretext

To execute this phase of the assessment, we utilized a pretext centered around the distribution of a fake cybersecurity awareness training document. Since the IT Helpdesk was on point with their Vishing awareness, our team figured that trying to leverage their awareness against them could prove to be effective. To further improve the effectiveness, we utilized an SMTP relay vulnerability on the Exchange server to send the email as the Directory of IT (See RAKMS-008). The pretext email, which can be seen below, was crafted to encourage recipients to interact with the attached Word document:



Mandatory Online Security Training - Action Required

Helena Kendall <hkendall@corp.kkms.local>
Today, 10:20 AM
Mark Magnolia

Reply all

This message was sent with high importance.

RAKMS_Security_Trainin...
115 KB

Download

Dear Parsleigh Calder,

You are receiving this email due to recent attempts of phishing on your account. Please complete the following training as soon as possible.

At Robert A Kalka Metropolitan Skyport (RAKMS), we take online security very seriously. To ensure the safety and security of our organization and your personal information, we are conducting a mandatory online security training session.

Training Details:

Title: Online Security Training

Duration: Approximately 30 minutes
Purpose: Enhancing your awareness of online security threats and best practices.
Deadline for Completion: Within 48 hours.

Instructions:
In order to protect the safety and security of our organization and comply with GDPR, RAKMS leverages RSA encrypted Word documents that must be decrypted to view the contents of on some computers for safe viewing.

1. Please download the attached document: 'RAKMS_Security_Training_Guide.doc'

2. Right-click the file and select properties, if the following message is listed at the bottom of the properties window, check 'Unblock' and click 'Apply', then close the window.

3. Open the document, if the document shows a message stating that it is encrypted, follow the instructions at the top of the document to decrypt the encrypted document.

4. Complete the training exercises included in the document.

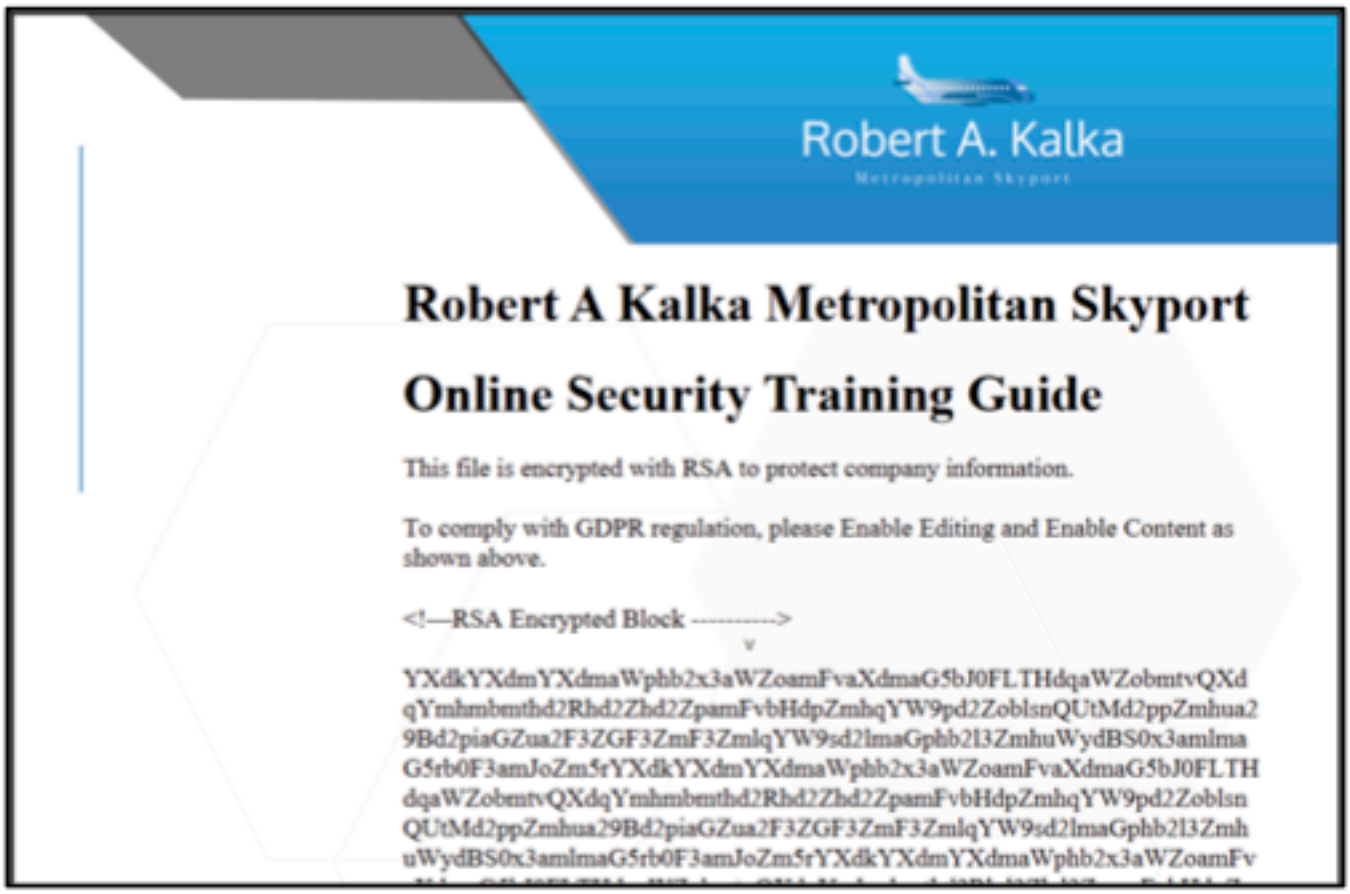
We understand the importance of online security in today's digital age, and your participation in this training is crucial in safeguarding our organization's data and your personal information.

Thank you for your cooperation in maintaining a secure online environment at RAKMS.

Phishing email

Embedded Macro Payload

The Word document attached to the phishing email contained a concealed threat in the form of embedded macros. The macros were designed to execute malicious code when the document was opened and enabled by the recipient. This approach allowed us to simulate a real-world scenario where attackers might exploit unsuspecting users by enticing them to enable macros, thereby compromising their systems. In order to do this, we created a document that appeared to be encrypted in such a way that enabling macros was a requirement to view the document.



Phishing email Doc

Finals-XX configured the macros on the document so that they would automatically trigger as soon as they were allowed to run. This was done via the Document_Open() function, with the AutoOpen() function also being configured to serve as redundancy. These functions were then called Finals-XX's custom function, which detected if the system was running a 32-bit or 64-bit version of Windows and downloaded and executed stage two from our Kali VM accordingly, giving us access to the system. In addition to this, it also replaces the content of the document with information that matches the pretext described in the email to reduce suspicion.

However, once again, there was never a callback to the listener setup to process the phishing email. The security training for RAKMS employees seems to have been a successful campaign.

Appendix B - Vulnerability Scales

Risk Rating Classifications

- Vulnerabilities that could be easily exploited by a remote unauthenticated attacker and lead to system compromise without requiring user interaction; exploits of these vulnerabilities are being actively used in the wild.
- Recommended remediation timeframe: Immediately

- Vulnerabilities that could allow local users to escalate privileges, allow unauthenticated remote users to view resources that should require authentication, allow authenticated remote users to execute arbitrary code, or allow remote users to cause a denial-of-service (DoS).
- Recommended remediation timeframe: 1-3 Months

- Vulnerabilities that may be difficult to exploit but could still lead to some compromise of the confidentiality, integrity, or availability of resources; these vulnerabilities could have a critical or high impact, but exploitation depends on technical expertise or unlikely system configurations.
- Recommended remediation timeframe: 3-12 Months

- Vulnerabilities in which successful exploitation requires extensive time and resources or where a successful exploit would have minimal business impact.
- Recommended remediation timeframe: As Needed

- An informational finding is a classification given to certain observations or data points that don't directly represent vulnerabilities or immediate security risks but provide valuable information to the organization about its security posture.
- Recommended remediation timeframe: As Part of Maintenance

Exploitation Likelihood Classifications

Level	Description
Likely	Exploitation is well-known and needs few public tools.
Possible	Exploitation is more common and can be carried out with common public tools.
Unlikely	Exploitation requires extensive knowledge of the system and the exploit.

Business Impact Classifications

Level	Description
Severe	A successful exploitation may result in major disruptions or outages of business-critical services.
Moderate	A successful exploitation of the vulnerability may cause significant long disruptions of services.
Mild	A successful exploitation of the vulnerability may affect some users and cause mild business disruptions.

Remediation Difficulty Classification

Level	Description
Hard	Remediation may require extensive reconfiguration of systems and may affect production.
Medium	Remediation may require small reconfigurations or require time-consuming or costly additions.
Easy	Remediation can be accomplished quickly and has a low difficulty level.

Appendix C - Open Source Intelligence

Employee Information

Based on the public-facing information on RAKMS online, Finals-XX was able to construct a rough organizational chart of a select number of their 201-500 employees (per LinkedIn about page). Specifically those of the information technology and public relations departments of RAKMS.

Associated Domains

During our enumeration of RAKMS' digital footprint, Finals-XX encountered three separate domains that were connected to a website claiming to be RAKMS'.

Domain	Description	Domain Registrant
kkms.us	Main site that the other two domains were/are mirroring.	Jason Ross Rochester, NY
liturgy.link	A former mirror of kkms.us that no longer shows a website.	Registration Private
essotrc.tricelogic.com	Exists as a redirect to kkms.us, routing any user visiting it onto the main site.	Registration Private

RAKMS' Interest in AI

RAKMS recently expressed interest in AI applications for the travel industry through a posted update on Linkedin. This underscores the possibility of encountering AI systems during our testing, which presents an opportunity to assess their vulnerabilities and potentially manipulate them to extract confidential information.

Robert A Kalka Metropolitan Skyport posted this • 1mo

That feeling when you read a leading consulting report and their recommendations have been part of your strategic plan for years ..... 😁

What AI means for travel—now and in the future

mckinsey.com • 15 min read

LinkedIn post

Appendix D - Tools Used

Reconnaissance Tools

AWS CLI	
Description	The AWS Command Line Interface (AWS CLI) is a set of open-source command-line tools provided by Amazon Web Services (AWS) for interacting with AWS services. AWS CLI can be leveraged to assess and enumerate security vulnerabilities within an AWS environment by enabling testers to query and manipulate AWS resources, identify misconfigurations, and assess the overall security posture of the cloud infrastructure from a command-line interface.
Source	https://aws.amazon.com/cli/

Bloodhound	
Description	BloodHound is a security tool designed for Active Directory environments. It assists penetration testers in visualizing and analyzing relationships within the network, helping identify potential attack paths and security risks for effective privilege escalation.
Source	https://github.com/BloodHoundAD/BloodHound

Enum4Linux	
Description	Enum4Linux is a tool specifically crafted for penetration testers to gather information from Windows and Samba systems during security assessments. It aids in the enumeration of user accounts, shares, and other valuable data, facilitating the identification of potential vulnerabilities in a network.
Source	https://www.kali.org/tools/enum4linux/

Feroxbuster	
Description	Feroxbuster is a web directory and file brute-force scanner designed for penetration testing. It helps security professionals discover hidden files and directories on web servers by efficiently and recursively

	searching for potential entry points, aiding in vulnerability assessments.
Source	https://github.com/epi052/feroxbuster

Gobuster	
Description	Gobuster is a command-line tool used for directory and file brute-forcing on web servers. It helps penetration testers discover hidden paths and files by making requests to the server and analyzing the responses, facilitating comprehensive web application security assessments.
Source	https://github.com/OJ/gobuster

LinWinPwn	
Description	LinWinPwn is a bash script that automates a number of Active Directory Enumeration and Vulnerability checks. The script uses a number of tools and serves as wrapper of them. Tools include: impacket, bloodhound, netexec, enum4linux-ng, ldapdomaindump, lsassy, smbmap, kerbrute, adidnsdump, certipy, silenthound, and others.
Source	https://github.com/lefayjey/linWinPwn

Nikto	
Description	Nikto is an open-source web server scanner that assists penetration testers in identifying potential vulnerabilities and security risks in web applications. It performs comprehensive checks for known issues and misconfigurations, aiding in the assessment of a website's security posture.
Source	https://github.com/sullo/nikto

Nmap	
Description	Nmap (Network Mapper) is a versatile and powerful network scanning tool used by penetration testers to discover hosts, services, and vulnerabilities on a network. It provides detailed information about open ports, running services, and other critical data for

	assessing the security of a networked environment.
Source	https://nmap.org/

NmapAutomator	
Description	Nmap Automator is a script designed to automate common tasks and enhance the usability of the Nmap security scanner. It simplifies the process of running Nmap scans with predefined configurations, making it easier for security professionals and penetration testers to conduct network reconnaissance and vulnerability assessments. Nmap Automator provides a user-friendly interface and organizes scan results for efficient analysis during security assessments.
Source	https://github.com/21y4d/nmapAutomator

Wappalyzer	
Description	Wappalyzer is a browser extension and command-line tool used for web application fingerprinting during penetration testing. It identifies the technologies and frameworks utilized by a website, providing valuable insights for security assessments by revealing the software stack, plugins, and potential vulnerabilities.
Source	https://www.wappalyzer.com/

Exploitation Tools

Burp Suite	
Description	Burp Suite is a comprehensive cybersecurity tool designed for web application security testing. It combines various functionalities, including scanning, crawling, and testing for vulnerabilities like SQL injection and cross-site scripting. Burp Suite facilitates manual and automated testing, making it a powerful asset for penetration testers and security professionals.
Source	https://www.kali.org/tools/burpsuite/

Certify / Certipy

Description	Certipy is an offensive tool for enumerating and abusing Active Directory Certificate Services (AD CS).
Source	https://github.com/ly4k/Certipy

Evil-WinRM	
Description	Evil-WinRM is a powerful Ruby script that enables penetration testers to interact with Windows machines remotely. It utilizes the Windows Remote Management (WinRM) service, providing a command-line interface for post-exploitation tasks and lateral movement during security assessments.
Source	https://github.com/Hackplayers/evil-winrm

Kerbrute	
Description	Kerbrute is a tool used by security professionals for assessing Kerberos vulnerabilities in Windows environments, enabling various attacks to identify potential weaknesses in authentication.
Source	https://github.com/ropnop/kerbrute

Netexec	
Description	NetExec (a.k.a nxc) is a network service exploitation tool that helps automate assessing the security of large networks.
Source	https://github.com/Pennyw0rth/NetExec

Metasploit / Msfvenom	
Description	Metasploit is a tool used for testing and executing exploits on computer systems. Msfvenom, part of Metasploit, specifically helps create customized payloads for delivering malicious code during security assessments.
Source	https://docs.metasploit.com/ https://docs.metasploit.com/docs/using-metasploit/basics/how-to-use-msfvenom.html

Rubeus	
Description	Rubeus is a powerful tool commonly used in penetration testing and red teaming. It focuses on Kerberos ticket manipulation within Windows environments, allowing security professionals to extract, create, and manipulate Kerberos tickets for various attacks such as ticket extraction, pass-the-ticket (PTT), and ticket renewal.
Source	https://github.com/GhostPack/Rubeus

SQLmap	
Description	SQLmap is an open-source penetration testing tool that automates the process of detecting and exploiting SQL injection vulnerabilities in web applications. It provides a range of options for database fingerprinting, data retrieval, and potentially even database takeover, making it a valuable tool for security professionals assessing the security of web applications.
Source	https://github.com/sqlmapproject/sqlmap

Post-Exploitation Tools

Hashcat	
Description	Hashcat is a widely used open-source password recovery tool that excels in cracking password hashes. It supports various hashing algorithms and attack modes, making it a versatile choice for security professionals conducting password audits, penetration testing, or other tasks related to password security.
Source	https://hashcat.net/hashcat/

John The Ripper	
Description	John the Ripper, often abbreviated as "John," is a popular open-source password cracking tool. It is used by security professionals and penetration testers to identify weak passwords by performing dictionary attacks, brute-force attacks, and various other password cracking techniques. John the Ripper supports a wide range of

	password hash algorithms and is known for its efficiency in password auditing.
Source	https://github.com/openwall/john

Mimikatz	
Description	Mimikatz is a powerful post-exploitation tool commonly used in penetration testing and security assessments. It specializes in extracting plaintext passwords, hashes, and Kerberos tickets from memory, enabling security professionals to perform credential theft and lateral movement within Windows environments. It's a valuable tool for demonstrating the vulnerabilities associated with credential handling in security evaluations.
Source	https://github.com/ParrotSec/mimikatz

Peass-ng	
Description	Privilege escalation tools for Windows and Linux/Unix* and MacOS. These tools search for possible local privilege escalation paths that you could exploit and print them to you with nice colors so you can recognize the misconfigurations easily.
Source	https://github.com/carlospolop/PEASS-ng

Sharphound	
Description	SharpHound is a post-exploitation tool specifically designed for Active Directory environments. It assists penetration testers in collecting detailed information about the Active Directory infrastructure, including users, groups, permissions, and trust relationships. SharpHound aids in identifying security vulnerabilities and potential attack paths within the network.
Source	https://github.com/BloodHoundAD/SharpHound

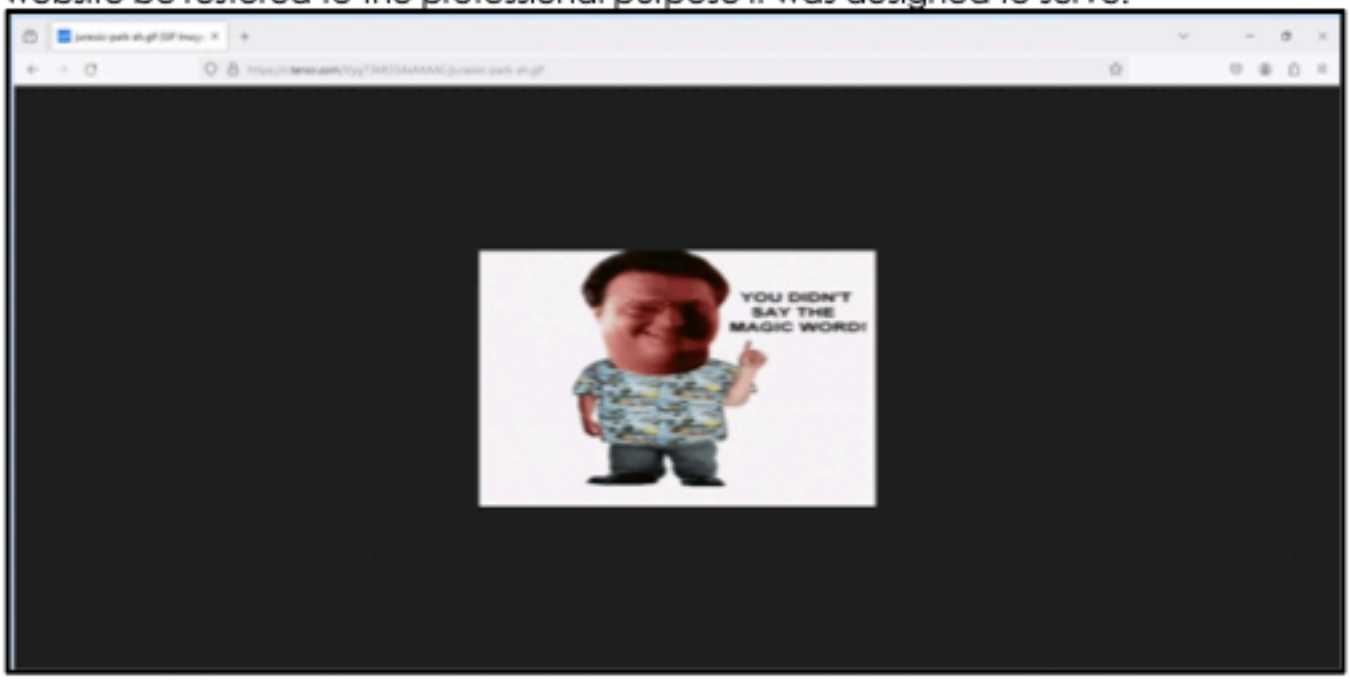
XRDP	
Description	XRDP is an open-source implementation of the Remote Desktop Protocol (RDP) that allows users to connect to a graphical desktop of a remote system over a network. It enables remote access to Linux

	systems using the same protocol commonly associated with remote desktop access in Windows environments.
Source	https://github.com/neutrinolabs/xrdp

Appendix E - Defacement of Website

RAKMS-Guest-Wifi.guest.kkms.local

The website hosted on the RAKMS-Guest-Wifi Linux box (10.0.200.5) had a very unprofessional and likely unauthorized GIF that appeared when you clicked "Accept" on the wifi Terms and Conditions. It is strongly recommended that this website be restored to the professional purpose it was designed to serve.



Defacement image displayed when a user agrees to the terms and conditions

Appendix F - Social Engineering Phone Call

Scope

Target: pcalder@corp.kkms.local
Department Called: IT Helpdesk
Call Time: 5 Minutes

Strategies

1. **Urgency and Panic:**
    - Started the call with urgency, expressing an immediate need for help.
    - Claimed the necessity for account access before an upcoming meeting.
2. **Familiarity Exploitation:**
    - Used email (pcalder@corp.kkms.local) as the basis for presenting last name and beginning letter of last name.
3. **Emotional Manipulation:**
    - Attempted to evoke sympathy and urgency by stating job dependence on the meeting.
    - Intensified urgency by having colleagues call out for the impersonated user during the call.

Call Notes from assigned Penetration Tester

"Upon calling helpdesk I was greeted and asked for what I need. I began with a frantic attitude, stating that I need help immediately accessing my account. I was then asked what my name was. Due to limited information at the time I replied "P Calder", and was then asked what happened. I stated in a panic that I tried using my username and password and wasn't able to log in, then cut myself off by saying that I had a meeting shortly and that I needed access immediately. The helpdesk individual assisting mentioned that I didn't sound right, and that he had worked with Parsleigh Calder before. I broke down and said that my job depended on the meeting and that I needed help getting access to the account immediately. Two of my colleagues called out asking for me immediately to add tension.

Individual I was impersonating entered the room, failure to gather any data. End of Call."

Appendix G - Bug Bounty Boarding Pass

Summary

Our team was approached on Day 2 in the afternoon by the legal team after they were contacted by an individual claiming to have a bug bounty on the boarding passes that would expose PII using the boarding pass.

Contained in the barcode of the boarding pass is all of the information listed on the boarding pass. This data includes name, date, departing airport, destination airport, flight number, gate, seat number, and other encoded data we were unable to extract.

Based on the ticket generator AWS Lambda function, which takes SSN as a parameter, it is possible that the boarding pass also contains the customer's SSN in some encoded fashion, although it should be noted we were unable to confirm this at this time.