RAKMS Security Assessment Report

11 November 2023

Team #6

Executive Summary

Assessment Objectives

On November 11, 2023, Team 6 conduct a comprehensive penetration test under contract from Robert A. Kalka Metropolitan Skyport to evaluate their security posture. The primary goals of this assessment included:

1. Identify exploitable vulnerabilities and assess their risk to infrastructure and operations
2. Evalute the effectiveness of current security controls
3. Ensure compliance with relevant security standards
4. Outline immediate and long-term remediation actions

Key Findings

- Discovered a critical vulnerability in the Domain Controller in the corporate network, allowing us to gain full access to the entire corporate network
- The tram controls could be operated without authorization, allowing outside users to start and stop the tram
- The requisition form can be accessed without authorization, allowing unauthorized purchases to be made
- The Werkzeug development console was found to be enabled in production, potentially allowing for unauthorized access to the host machine

Business Impact

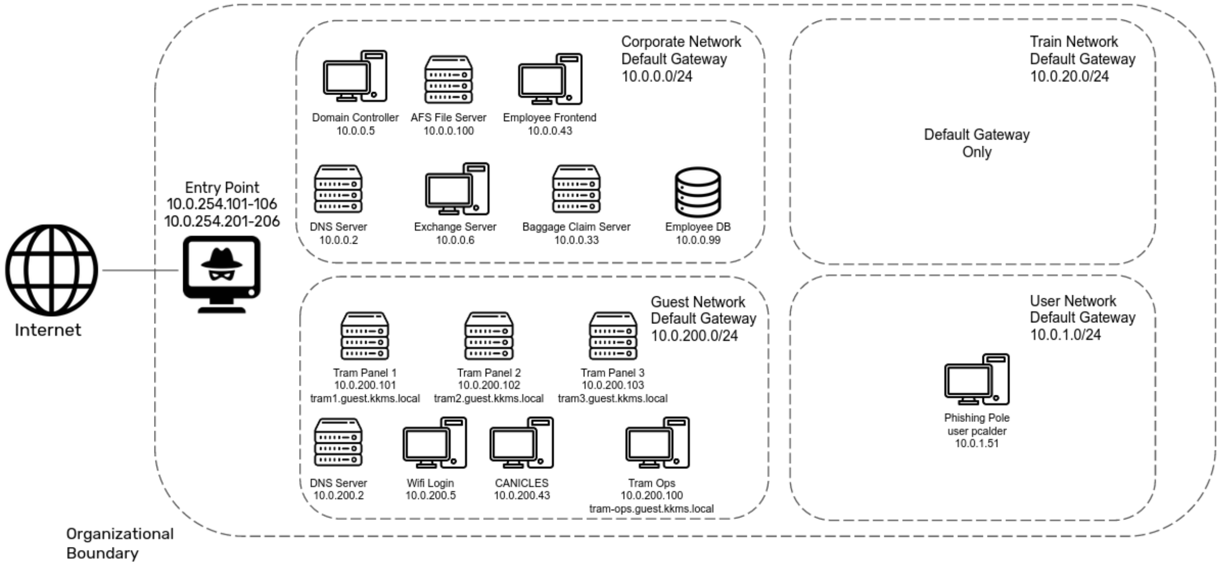
As a world-class airport serving thousands of passengers every day, Robert A. Kalka Metropolitan Skyport must prioritize securing their infrastructure through robust cybersecurity measures. Cyber attacks could lead to disruptions in critical operations, flight schedules, and air traffic management systems. This would result in decreased efficiency and service quality, a possible threat to public safety, and significant financial losses. Additionally, the airport may face regulatory penalties and compliance issues. A weak cybersecurity posture would undermine Robert A. Kalka Metropolitan Skyport's business resilience and competitiveness within the industry.

By engaging in a penetration test, RAKMS is showing impressive forethought and will undoubtedly be better-protected against malicious adversaries in the future. Although RAKMS's security is not perfect, security rarely is, and the steps that have already been taken to protect such critical infrastructure comprise an excellent foundation upon which a strong cybersecurity posture can be built.

Engagement Overview

Network Topology

Team 6 utilized network scanning tools to enumerate active machines on the network.



Scope

This engagement was performed assuming the perspective of an attacker with a connection to the airport’s internal networks. The scope included the network ranges 10.0.200.0/24 and 10.0.1.0/24. Team 6 identified a total of 15 hosts, comprised of Windows and Linux machines.

Timeline

To begin, all four networks were scanned as they were accessible from the given entry point. The vulnerability in the tram control panel was switfly discovered and permission to fire was requested from RAKMS representatives. After receiving approval, control was taken of the tram between 1:15 PM and 2:15 PM.

Soon afterwards, representatives from RAKMS identified an employee account to be used as a target for a phishing attack. After constructing a malicious payload, we sent it to the user using the Guest account available by default in Exchange. The user downloaded and executed the malicious file, and control over the user’s workstation was attained.

Subsequently, we focused on the corporate network as it appeared to contain more critical targets. The Domain Controller was found to be vulnerable, and was compromised shortly thereafter. From there, the Exchange server and Microsoft SQL server on the corporate network were also fully compromised and taken over, allowing complete access to user account credentials and data.

Methodology

All testing was performed in accordance with the Penetration Testing Execution Standard (PTES), a standardized framework for executing penetration tests. Team 6 followed the defined stages: pre-engagement interactions, intelligence gathering, threat modeling, vulnerability analysis, exploitation, post exploitation, and reporting.[1] In pre-engagement, Team 6 and Robert A. Kalka Metropolitan Skyport established goals, scope, and rules for the testing. Then, passive and active reconnaissance was conducted to gather information about the target systems. Team 6 subsequently identified potential threats, analyzed and exploited vulnerabilities, and further escalated privileges where possible. After the engagement was concluded, the results and findings were documented and remediations were recommended accordingly.

Risk assessments were performed in accordance with the Common Vulnerability Scoring System (CVSS), a standardized framework to assess and numerically classify the severity of security vulnerabilties. Vulnerabilities are evaluated based on exploitability, scope, impact, and environmental or temporal metrics. The combined scores of each metric result in an overall CVSS score from 0.0 to 10.0, with higher scores indicating greater risk. This score maps to a predefined security level, either Critical, High, Medium, or Low, which aids in the prioritization of responses to vulnerabilities.[2]

Severity	**Base Score Range**
Critical	9.0 - 10.0
High	7.0 - 8.9
Medium	4.0 - 6.9
Low	0.1 - 3.9
None	0.0

Positive Security Measures

Listed below are the positive observations we made while conducting the vulnerability assessment.

- No default nor easily crackable passwords in SSH servers, SQL databases, or Mimikatz memory dump
- The Linux servers ran mostly up-to-date software
- Attentitive and quick to respond to technical issues

Strategic Recommendations

Immediate Remediation

Operational

1. Instantiate a user training program to help corporate employees identify phishing and malware emails; this will reduce the frequency and effectiveness of phishing attacks.
2. Audit terms and conditions page visible to public.

Technical

1. Take steps to split essential services among multiple hosts, rather than hosting multiple services on a single host.
2. Update all public-facing software, including:
    a. Rails/Ruby on the TramOps server (10.0.200.100).
    b. OpenSSH on multiple Ubuntu servers in the Corporate and Guest networks
    c. Exchange (10.0.0.6) is wildly out of date (2007).
    d. Nginx 1.18 on the CANICLES server (10.0.200.43) and Tram Panels (10.0.200.101-10.0.200.103).
3. Take steps to restrict access to the User and Train networks from the Guest network.

Long-term Remediation

Operational

1. Invest in professional development programs for IT personnel; this will result in improved security posture and a more resilient and defensible network.
2. Regularly assess the security of RAKMS infrastructure by contracting the services of penetration testers or other white-hat security professionals.

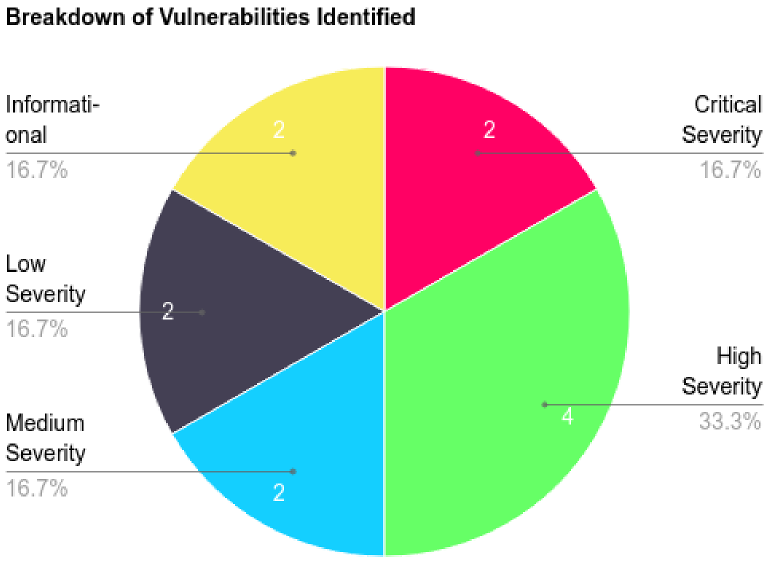
Technical

1. Regularly ensure the latest OS updates and security patches are installed on all systems.
2. Install antimalware and monitoring software on all host machines to ensure malicious binaries cannot be downloaded or executed.
3. Review cybersecurity frameworks such as NIST and CIS CSC and audit new and existing systems to ensure compliance with the latest and mot secure configurations for company systems.

Technical Findings

Overview

Vulnerability findings by severity:



Overview of Vulnerabilities:

ID	Name	Machine	CVSS Score
C1	EternalRomance/EternalSynergy/Eternal Champion SMB Remote Code Execution – MS17-010	SkyControl-01 (10.0.0.5:445)	9.9 (Base CVE 8.1)
C2	Tram Control Unauthorized Access	Trams (10.0.200.101-103)	9.6
H1	Hidden Requisition Form Unauthorized Access	AWS Environment	8.2
H2	Werkzeug Development Console Enabled in Production	Trams (10.0.200.101-103)	8.1

H3	Kerberos (Mis)configuration	SkyControl-01 (10.0.0.5)	7.4
H4	LDAP Information Disclosure	SkyControl-01 (10.0.0.5)	7.1
M1	No Lockout Mechanism for Repeated Login Failures	Employee Database (10.0.0.43)	6.5
M2	Website Directory Contents Available	Flight List (10.0.0.100:7000)	4.5
L1	Data API Publicly Available	AWS	3.0
L2	Employee Database Admin Curlable	Employee Database (10.0.0.43)	2.0
I1	EternalBlue – CVE-2017-0144	Domain Controller SkyControl-01 (10.0.0.5:445)	0.0
I2	DoubleTap Rails Vulnerability	TramOps (10.0.200.100:3000)	0.0

Critical

C1	EternalRomance/EternalSynergy/EternalChampion SMB Remote Code Execution – MS17-010	SkyControl-01 (10.0.0.5:445)	9.9 (Base CVE 8.1)

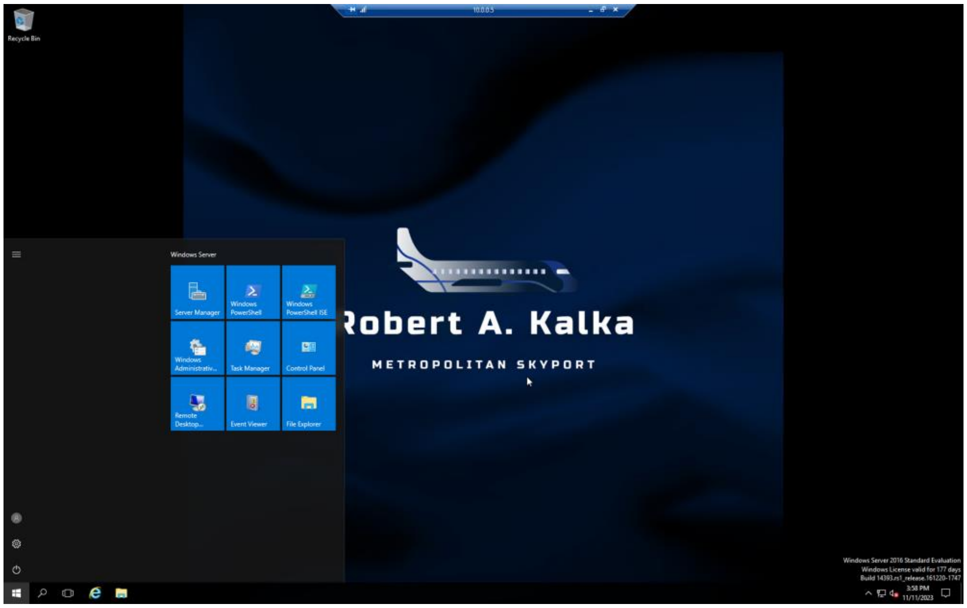
Scope

This vulnerability affects the Domain Controller SkyControl-01, at 10.0.0.5 on port 445.

Likelihood of Exploitation

High likelihood of exploitation. The existence of a well-known vulnerability, which is easily exploitable with a metasploit module, allows for low skill exploitation of the "psexec" vulnerability. The presence of an out-of-date SMB server (in this case, SMBv1, a known insecure SMB version) will make psexec one of the first tools reached for in an attacker's toolbox.

Proof of Compromise



Impact

Critical. Access to the Domain Controller with a Local Administrator account allows for access to the most important machine on the network. It would be very easy for the attacker to put measures in place to stay on the network for a long period of time. In addition, the presence of the authentication mechanism of Kerberos on the system allowed the use of malware called Mimikatz to gain the highest level of privilege in the Domain. The escalated privileges allows access to any other systems on the Domain.

The business implications of an attack like this would be devastating. With such a powerful machine on the network being control of the attacker, a malicious entity could modify, destroy, and/or add anything they wished onto the network. As a result, important business data, company information, employee information, client information, and operation of all Windows servers and machines on the entire domain are at risk. Put simply, the business impact is at a maximum with this vulnerability, and absolutely MUST be addressed.

Remediation

Use an up-to-date SMB server, and avoid hosting it on the Domain Controller. In addition, Kerberos should almost always be on its own system isolated from any other points of failure. Reduce any and all traffic on the Kerberos machine that is not required for its operation, and ensure only Administrators have access to it.

References

https://nvd.nist.gov/vuln/detail/CVE-2017-0147
https://nvd.nist.gov/vuln/detail/CVE-2017-0143
https://nvd.nist.gov/vuln/detail/CVE-2017-0146
https://blog.quest.com/kerberos-authentication-how-it-works-and-how-to-maximize-its-security/

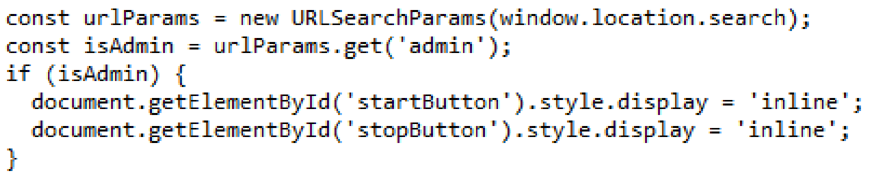
C2	Tram Control Unauthorized Access	Trams (10.0.200.101-103)	9.6

Scope

This vulnerability affects the Tram Control Systems at 10.0.200.101-103.

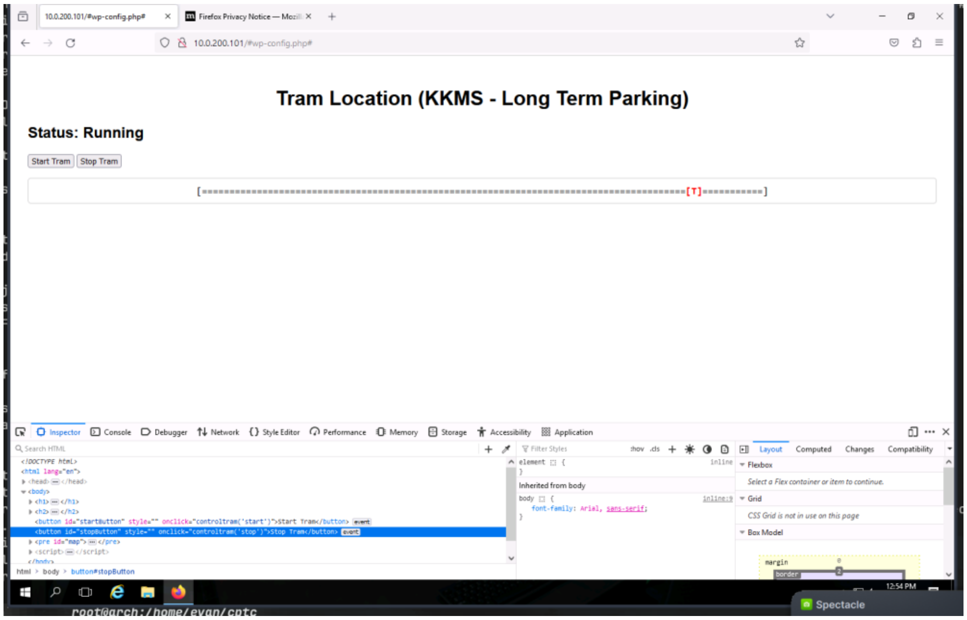
Likelihood of Exploitation

The likelihood of exploitation for this vulnerability is very high. Once on the page, the end user is confronted with a simple GUI which depicts where the tram is. However, upon further inspection of the site, a tram control panel exists as well.
The admin privilege is bypassed very easily by accessing them in the page's source. These can then easily be unhidden, and interacted with.



```
const urlParams = new URLSearchParams(window.location.search);
const isAdmin = urlParams.get('admin');
if (isAdmin) {
  document.getElementById('startButton').style.display = 'inline';
  document.getElementById('stopButton').style.display = 'inline';
}
```

Proof of Compromise



Tram Location (KKMS - Long Term Parking)

Status: Running

Start Tram | Stop Tram

```
[====================================================================================[T]==========]
```

```
<!DOCTYPE html>
<html lang="en">
  <head> … </head>
  <body>
    <h1> … </h1>
    <h2> … </h2>
    <button id="startButton" style="" onclick="controltram('start')">Start Tram</button> event
    <button id="stopButton" style="" onclick="controltram('stop')">Stop Tram</button> event
    <pre id="map"> … </pre>
    <script> … </script>
  </body>
```

```
element { } inline
Inherited from body
body {
  font-family: Arial, sans-serif;
} inline:9
```

10.0.200.101/#wp-config.php#
Firefox Privacy Notice — Mozil
10.0.200.101/#wp-config.php#
Inspector
Console
Debugger
Network
Style Editor
Performance
Memory
Storage
Accessibility
Application
Search HTML
Filter Styles
Layout
Computed
Changes
Compatibility
Flexbox
Select a Flex container or item to continue.
Grid
CSS Grid is not in use on this page
Box Model
margin
border
html > body > button#stopButton
12:54 PM
Spectacle
root@arch:/home/evan/cptc

Impact

Critical. This attack has extreme business consequences. With the power to control the stopping and starting of the tram, the attacker can effectively cause a dangerous interruption of service, either completely restricting the tram's ability to move or even forcing it to never stop, thereby trapping the clientele. This would result in terrible events such as endangerment of customers, fines, extreme loss of reputation, and loss of revenue both in the short and long term.

Remediation

Enable access controls so that only certain authorized users can access this page. Calls to the API to stop and start this tram must go through access control checks so that only those who are strictly allowed to control the trams may use this functionality.

References

https://csrc.nist.gov/pubs/sp/800/82/r3/final
https://csrc.nist.gov/pubs/sp/800/44/ver2/final
https://www.cisecurity.org/controls/application-software-security

High

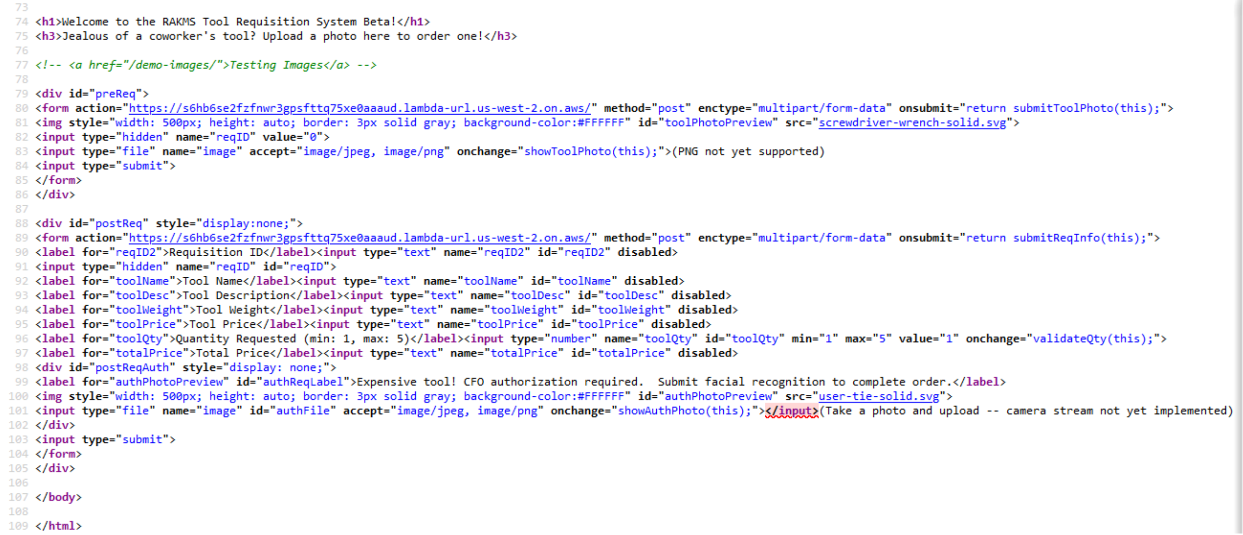
H1	Hidden Requisition Form Unauthorized Access	AWS	8.2

Scope

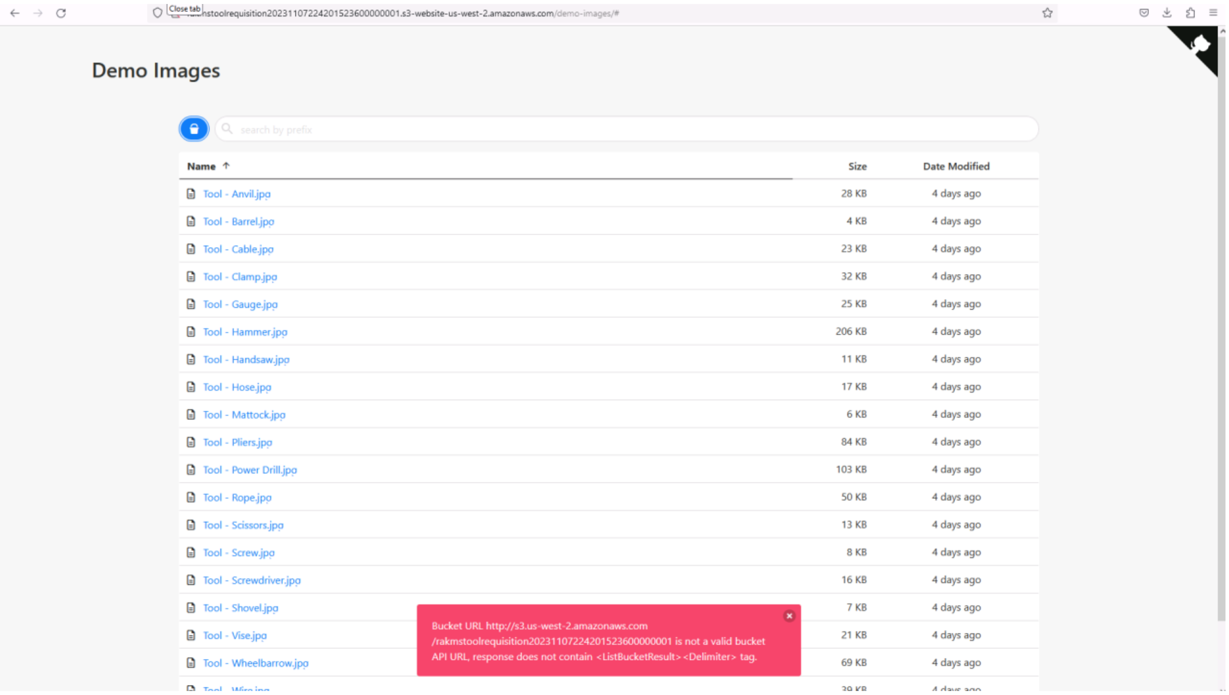
This vulnerability affects the following AWS environment:
http://rakmstoolrequisition20231107224201523600000001.s3-website-us-west-2.amazonaws.com/

Likelihood of Exploitation

Somewhat likely. In the case that an attacker finds this AWS endpoint, it is near-trivial to exploit this vulnerability. The attacker needs to simply access the source and view the /demo-tools endpoint.



```html

<h1>Welcome to the RAKMS Tool Requisition System Beta!</h1>
<h3>Jealous of a coworker's tool? Upload a photo here to order one!</h3>

<!-- <a href="/demo-images/">Testing Images</a> -->

<div id="preReq">
<form action="https://s6hb6se2fzfnwr3gpsfttq75xe0aaaud.lambda-url.us-west-2.on.aws/" method="post" enctype="multipart/form-data" onsubmit="return submitToolPhoto(this);">
<img style="width: 500px; height: auto; border: 3px solid gray; background-color:#FFFFFF" id="toolPhotoPreview" src="screwdriver-wrench-solid.svg">
<input type="hidden" name="reqID" value="0">
<input type="file" name="image" accept="image/jpeg, image/png" onchange="showToolPhoto(this);">(PNG not yet supported)
<input type="submit">
</form>
</div>

<div id="postReq" style="display:none;">
<form action="https://s6hb6se2fzfnwr3gpsfttq75xe0aaaud.lambda-url.us-west-2.on.aws/" method="post" enctype="multipart/form-data" onsubmit="return submitReqInfo(this);">
<label for="reqID2">Requisition ID</label><input type="text" name="reqID2" id="reqID2" disabled>
<input type="hidden" name="reqID" id="reqID">
<label for="toolName">Tool Name</label><input type="text" name="toolName" id="toolName" disabled>
<label for="toolDesc">Tool Description</label><input type="text" name="toolDesc" id="toolDesc" disabled>
<label for="toolWeight">Tool Weight</label><input type="text" name="toolWeight" id="toolWeight" disabled>
<label for="toolPrice">Tool Price</label><input type="text" name="toolPrice" id="toolPrice" disabled>
<label for="toolQty">Quantity Requested (min: 1, max: 5)</label><input type="number" name="toolQty" id="toolQty" min="1" max="5" value="1" onchange="validateQty(this);">
<label for="totalPrice">Total Price</label><input type="text" name="totalPrice" id="totalPrice" disabled>
<div id="postReqAuth" style="display: none;">
<label for="authPhotoPreview" id="authReqLabel">Expensive tool! CFO authorization required.  Submit facial recognition to complete order.</label>
<img style="width: 500px; height: auto; border: 3px solid gray; background-color:#FFFFFF" id="authPhotoPreview" src="user-tie-solid.svg">
<input type="file" name="image" id="authFile" accept="image/jpeg, image/png" onchange="showAuthPhoto(this);"></input>(Take a photo and upload -- camera stream not yet implemented)
</div>
<input type="submit">
</form>
</div>

</body>

</html>
```



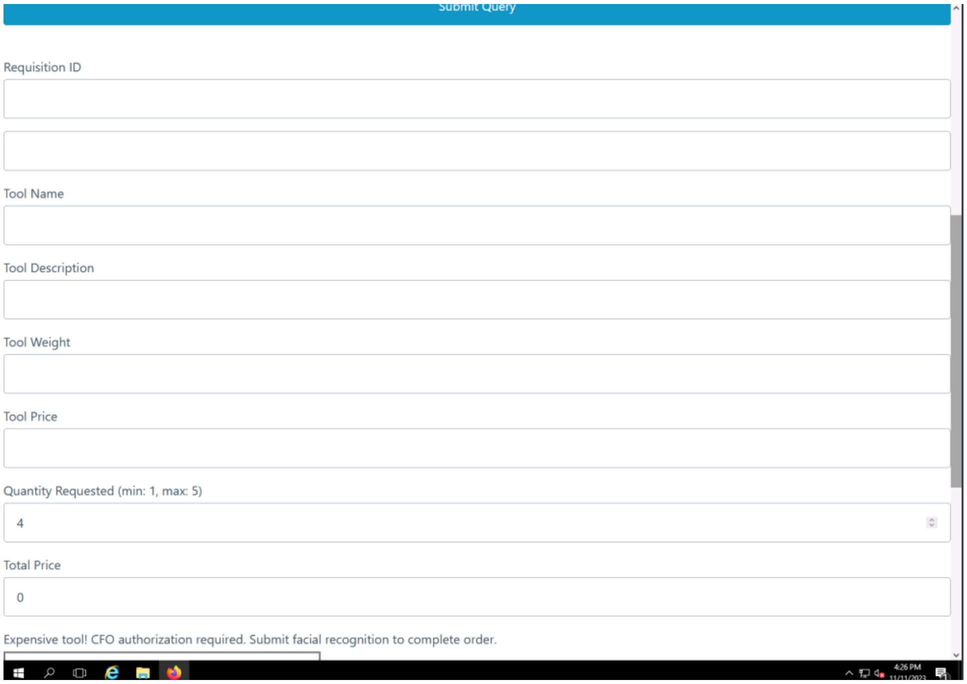
Close tab
rakmstoolrequisition20231107224201523600000001.s3-website-us-west-2.amazonaws.com/demo-images/#
search by prefix

Demo Images

Name ↑	Size	Date Modified
Tool - Anvil.jpg	28 KB	4 days ago
Tool - Barrel.jpg	4 KB	4 days ago
Tool - Cable.jpg	23 KB	4 days ago
Tool - Clamp.jpg	32 KB	4 days ago
Tool - Gauge.jpg	25 KB	4 days ago
Tool - Hammer.jpg	206 KB	4 days ago
Tool - Handsaw.jpg	11 KB	4 days ago
Tool - Hose.jpg	17 KB	4 days ago
Tool - Mattock.jpg	6 KB	4 days ago
Tool - Pliers.jpg	84 KB	4 days ago
Tool - Power Drill.jpg	103 KB	4 days ago
Tool - Rope.jpg	50 KB	4 days ago
Tool - Scissors.jpg	13 KB	4 days ago
Tool - Screw.jpg	8 KB	4 days ago
Tool - Screwdriver.jpg	16 KB	4 days ago
Tool - Shovel.jpg	7 KB	4 days ago
Tool - Vise.jpg	21 KB	4 days ago
Tool - Wheelbarrow.jpg	69 KB	4 days ago
Tool - Wire.jpg	39 KB	4 days ago

Bucket URL http://s3.us-west-2.amazonaws.com /rakmstoolrequisition20231107224201523600000001 is not a valid bucket API URL, response does not contain <ListBucketResult><Delimiter> tag.

From there, the attacker can copy one of the listed images, unhide the hidden submit button and related form inputs from the main page, and load the image into the image upload. Then, the necessary requisition data will be loaded, and the attacker can also choose to order more of the item as necessary. The attacker can then submit and purchase these items, completely free of any authorization checks.



Requisition ID

Tool Name

Tool Description

Tool Weight

Tool Price

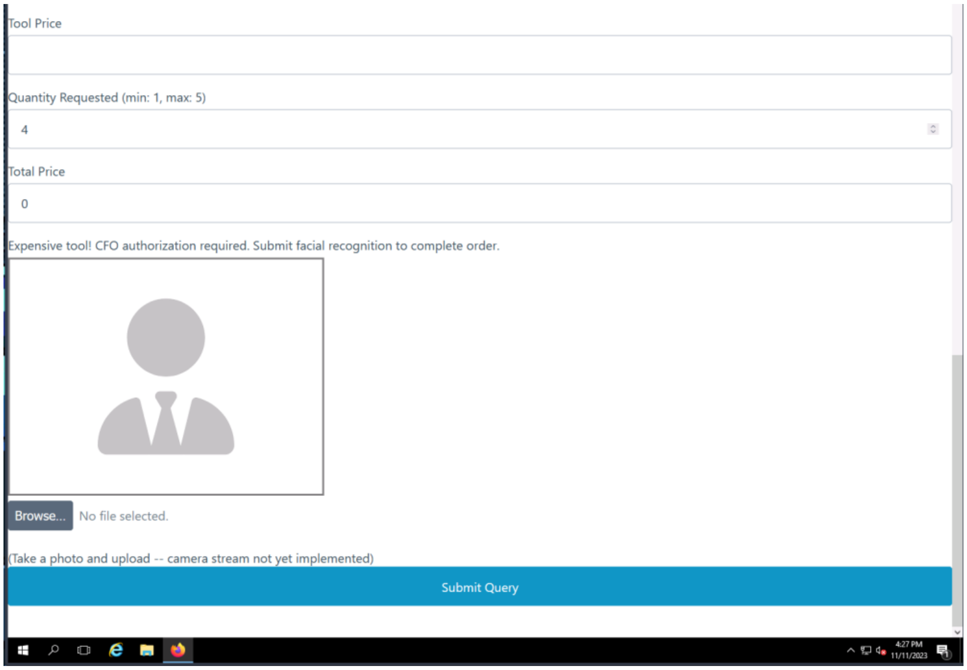
Quantity Requested (min: 1, max: 5)

4

Total Price

0

Expensive tool! CFO authorization required. Submit facial recognition to complete order.



Tool Price

Quantity Requested (min: 1, max: 5)

4

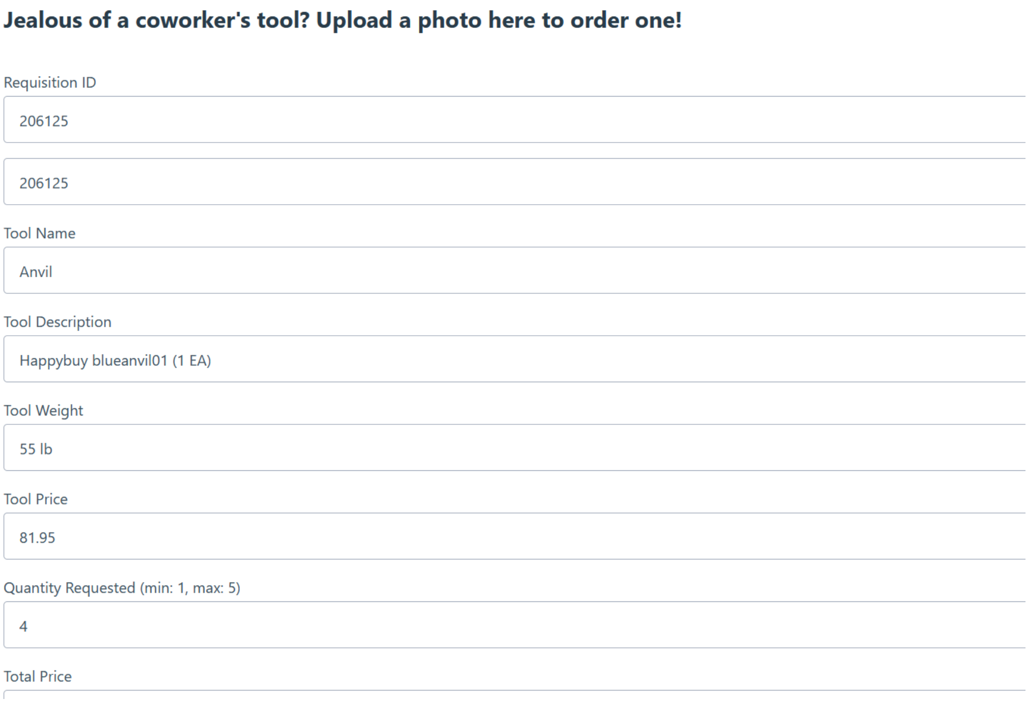
Total Price

0

Expensive tool! CFO authorization required. Submit facial recognition to complete order.

Browse... No file selected.

(Take a photo and upload -- camera stream not yet implemented)



Jealous of a coworker's tool? Upload a photo here to order one!

Requisition ID

206125

206125

Tool Name

Anvil

Tool Description

Happybuy blueanvil01 (1 EA)

Tool Weight

55 lb

Tool Price

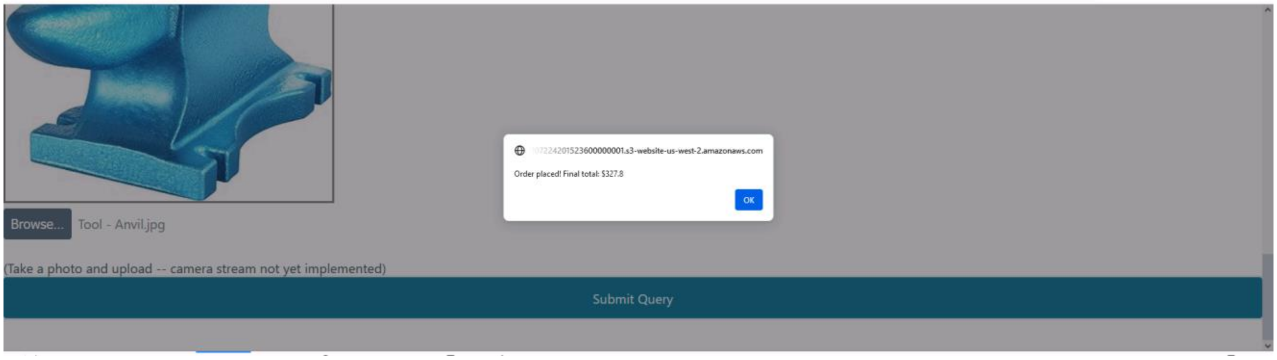
81.95

Quantity Requested (min: 1, max: 5)

4

Total Price

Proof of Compromise



107224201523600000001.s3-website-us-west-2.amazonaws.com

Order placed! Final total: $327.8

OK
Browse...
Tool - Anvil.jpg
(Take a photo and upload -- camera stream not yet implemented)
Submit Query

Impact

This vulnerability, when exploited, represents extreme business impact, since the attacker could order as many items as they want, thereby putting intense strain on the airport's financial reserves and undermining the trust of financial institutions in dealing with RAKMS. This could lead to financial issues that could inhibit the airport's daily operations. Additionally, the presence and functionality of this endpoint could allow attackers to derive information about AWS environments in use by RAKMS.

Remediation

If the page section is in beta, do NOT allow it to be shown on a production site. Implement access control checks to ensure that only authorized individuals may interact with this form in any capacity. Ideally, access to this webpage would be restricted to internal users only.

References

https://csrc.nist.gov/projects/access-control-policy-and-implementation-guides
https://csrc.nist.gov/pubs/sp/800/53/r5/upd1/final

H2	Werkzeug Development Console Enabled in Production	Trams (10.0.200.101-103)	8.1

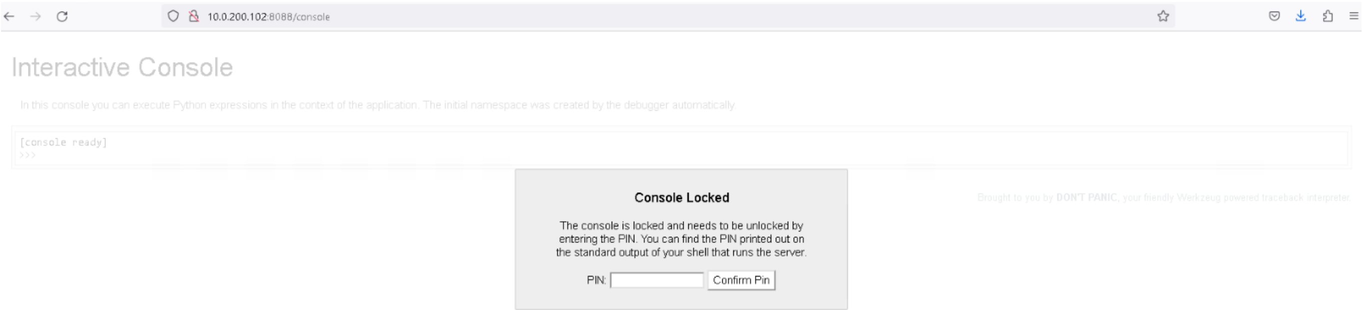
Scope

This vulnerability affects the Tram Control Systems at 10.0.200.101-103 on ports 80 and 8088.

Likelihood of Exploitation

Somewhat likely. In the event an attacker determines the server's software, the presence of a development mode, the portal for said development mode, and the pin to enable the terminal, they will be able to compromise the system. Discovering the console is trivial, but correctly guessing the pin is unlikely unless the pin is written down, simple, or is ever disabled.

Proof of Compromise



Interactive Console

In this console you can execute Python expressions in the context of the application. The initial namespace was created by the debugger automatically.

```
[console ready]
>>>
```

Brought to you by DON'T PANIC, your friendly Werkzeug powered traceback interpreter.

Console Locked

The console is locked and needs to be unlocked by entering the PIN. You can find the PIN printed out on the standard output of your shell that runs the server.

PIN: [ ] Confirm Pin

This should not be accessible publicly; see the References section for more information.

Impact

The allows for complete access to the machine through a Python shell and, by extension, any subprocess executed. Access to a local Python shell grants a foothold into the network and potentially a means to privilege escalation. Control over the trams could potentially be gained once access to the Python shell has been attained. This can have major business impact as the people movers may be prevented from starting, prevented from stopping, or even made to crash into each other. This could also lead to economic loss, both from lost revenue due to a lack of trust in the airport's safety as well as compensation paid to possibly injured passengers.

Remediation

Properly deploying the Werkzeug server using the recommended deployment methods as listed in the deployment guide on the Werkzeug documentation. The console should be disabled and debug mode should never be enabled in the production server.

References

Debugging info: https://werkzeug.palletsprojects.com/en/3.0.x/debug/#using-the-debugger
Proper deployment methods: https://werkzeug.palletsprojects.com/en/3.0.x/deployment/

H3	Kerberos (mis)configuration	SkyControl-01 (10.0.0.5)	7.4

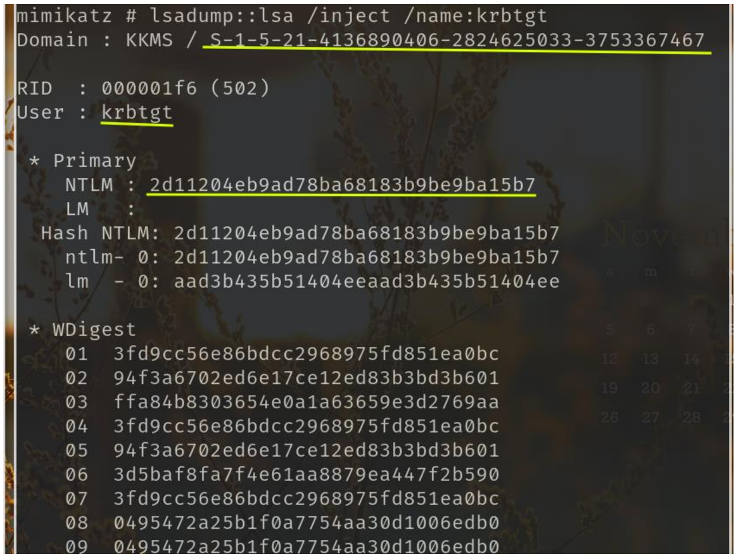
Scope

This misconfiguration affects the Domain Controller SkyControl-01, at 10.0.0.5 on port 88.

Likelihood of Exploitation

Individually, this misconfiguration is not entirely exploitable. However, given the high value and prominence of the related server, it can very easily lead to problematic conditions. Since the Domain Controller provides administrative services to the entire RAKMS domain, having it provide other endpoints (such as those relating to Kerberos) increases its attack surface and leaves it open as a pivot point.

Proof of Compromise



```
mimikatz # lsadump::lsa /inject /name:krbtgt
Domain : KKMS / S-1-5-21-4136890406-2824625033-3753367467

RID  : 000001f6 (502)
User : krbtgt

 * Primary
    NTLM : 2d11204eb9ad78ba68183b9be9ba15b7
    LM   :
  Hash NTLM: 2d11204eb9ad78ba68183b9be9ba15b7
    ntlm- 0: 2d11204eb9ad78ba68183b9be9ba15b7
    lm  - 0: aad3b435b51404eeaad3b435b51404ee

 * WDigest
    01  3fd9cc56e86bdcc2968975fd851ea0bc
    02  94f3a6702ed6e17ce12ed83b3bd3b601
    03  ffa84b8303654e0a1a63659e3d2769aa
    04  3fd9cc56e86bdcc2968975fd851ea0bc
    05  94f3a6702ed6e17ce12ed83b3bd3b601
    06  3d5baf8fa7f4e61aa8879ea447f2b590
    07  3fd9cc56e86bdcc2968975fd851ea0bc
    08  0495472a25b1f0a7754aa30d1006edb0
    09  0495472a25b1f0a7754aa30d1006edb0
```

Once having accessed the NT Authority/System by means of exploit C1 (documented above), we were able to generate a Kerberos ”golden ticket” and use that to gain complete control over the domain. Were the Kerberos services of the domain properly segregated into their own instances, this would not have been possible.

Impact

As documented above, having a service like Kerberos colocated with a critical service like the Domain Controller allows for a complete takeover of the network if a separate vulnerability leading to NT Authority\System access is found. This has a severe and critical impact, with the potential to entirely halt core business operations if an attacker takes over the network and decides to shut down the services on the network, and increases the attack surface of the entire network. The attack surface will expand to machines like the Exchange server at 10.0.0.6 and the BaggageClaim database at 10.0.0.43.

Remediation

Relocating the Kerberos service to a separate machine would reduce the attack surface on the Domain Controller, lengthening the minimum attack chain required to reach the Domain Controller (arguably the most critical component of the Windows domain).

References

https://blog.quest.com/kerberos-authentication-how-it-works-and-how-to-maximize-its-security/

H4	LDAP Information Disclosure	SkyControl-01 (10.0.0.5)	7.1

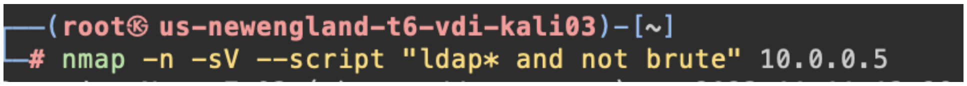
Scope

This information disclosure affects the Domain Controller SkyControl-01, at 10.0.0.5 on port 389.

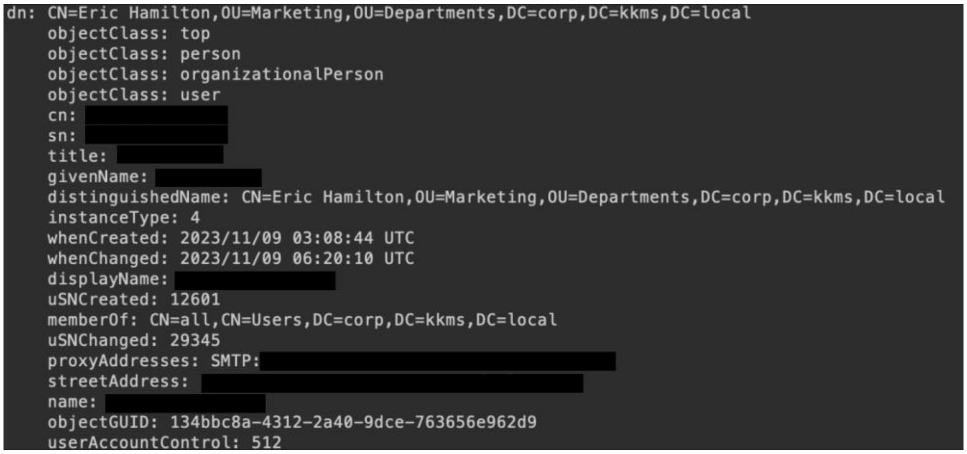
Likelihood of Exploitation

It is highly likely that an attacker could perform this exploit due to its ease of execution and the commonality of LDAP nmap scripts.

Proof of Compromise



```
┌──(root㉿ us-newengland-t6-vdi-kali03)-[~]
└─# nmap -n -sV --script "ldap* and not brute" 10.0.0.5
```



```
dn: CN=Eric Hamilton,OU=Marketing,OU=Departments,DC=corp,DC=kkms,DC=local
    objectClass: top
    objectClass: person
    objectClass: organizationalPerson
    objectClass: user
    cn: [redacted]
    sn: [redacted]
    title: [redacted]
    givenName: [redacted]
    distinguishedName: CN=Eric Hamilton,OU=Marketing,OU=Departments,DC=corp,DC=kkms,DC=local
    instanceType: 4
    whenCreated: 2023/11/09 03:08:44 UTC
    whenChanged: 2023/11/09 06:20:10 UTC
    displayName: [redacted]
    uSNCreated: 12601
    memberOf: CN=all,CN=Users,DC=corp,DC=kkms,DC=local
    uSNChanged: 29345
    proxyAddresses: SMTP:[redacted]
    streetAddress: [redacted]
    name: [redacted]
    objectGUID: 134bbc8a-4312-2a40-9dce-763656e962d9
    userAccountControl: 512
```

(user information has been redacted for reasons of privacy)

After running various LDAP scripts against the target system with nmap, sensitive personal information of employees was revealed. An attacker could learn about employee names, roles, their email address, and their street address.

Impact

Being able to access employee's personal data has a severe impact due to privacy violations and possible legal consequences. Leaking PII could jeopardize an employee's personal safety and put them at increased risk at identity theft. Furthermore, enumerating users and their work emails may give attackers valuable information to further attack the system, like knowing what user accounts to attempt brute-forcing or what email addresses to send phishing emails to.

Remediation

On the LDAP server, anonymous access should be disabled. Access controls should be strengthened, with proper authentication and authorization mechanisms for all connections.

References

https://serverfault.com/questions/63916/how-to-disable-anonymous-access-on-ldap

Medium

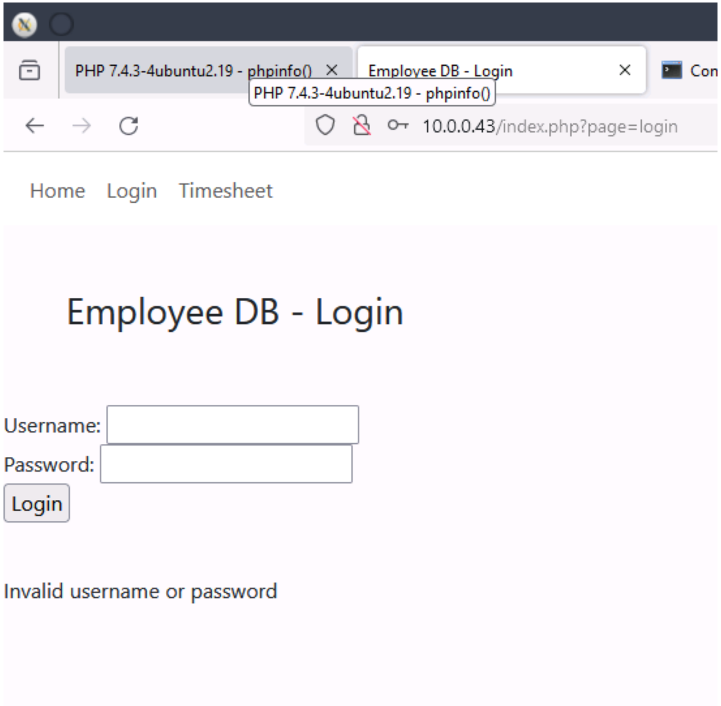
M1	No Lockout Mechanism for Repeated Login Failures	Employee Database (10.0.0.43)	6.5

Scope

This vulnerability affects the Employee Database at 10.0.0.43.

Likelihood of Exploitation

It is somewhat likely that a malicious actor exploits this vulnerability.


PHP 7.4.3-4ubuntu2.19 - phpinfo()
Employee DB - Login
Con
PHP 7.4.3-4ubuntu2.19 - phpinfo()
10.0.0.43/index.php?page=login
Home
Login
Timesheet
Login

Employee DB - Login

Username:
Password:

Invalid username or password

The web server only returns an “Invalid username or password,” but does NOT lock out the end user after repeated failed attempts. Thus, the attacker may guess as many username and password combinations as they wish; in the case that they know of a certain username or have an extensive wordlist, a brute force attack is trivial.

Proof of Compromise

Due to time constraints and limitations of the underlying infrastructure, we chose not to exploit this vulnerability as it could easily lead to degraded service for employees of RAKMS.

Impact

The technical and business impacts of this exploit are significant. In the case that an attacker successfully brute forces a privileged account, they may be able to create and delete employee information in the database, resulting in major technical issues for the business – i.e. employees cannot access their accounts – which will impede daily necessary operations. Creation of new employees may act as a back door, i.e. an extra way for the attacker to get in later.

Remediation

Implement a lockout policy such that after a certain amount of failed password attempts (ex. 5 attempts), the end user is temporarily locked out. Furthermore, ensure that 2-factor authentication is used to ensure that the end user is an authorized entity.

References

https://www.nist.gov/itl/smallbusinesscyber/guidance-topic/multi-factor-authentication
https://www.cisecurity.org/controls/access-control-management

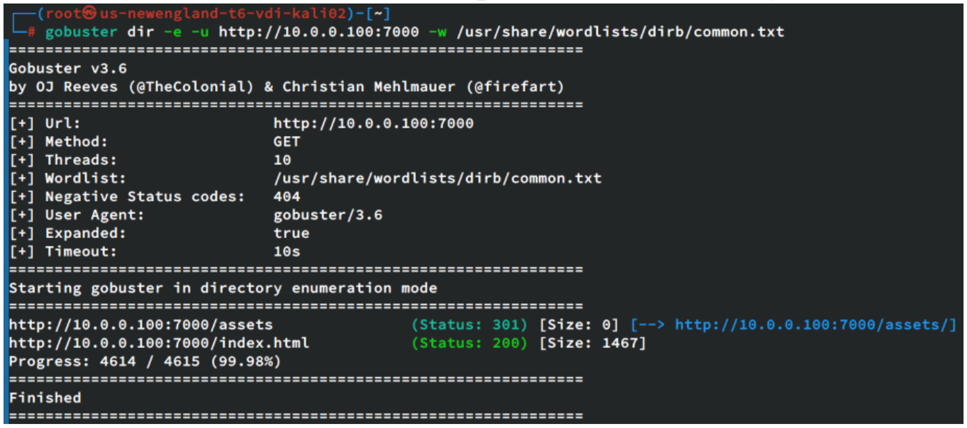
M2	Website Directory Contents Available	Flight List (10.0.0.100:7000)	4.5

Scope

This vulnerability affects the Flight List at 10.0.0.100 on port 7000.

Likelihood of Exploitation

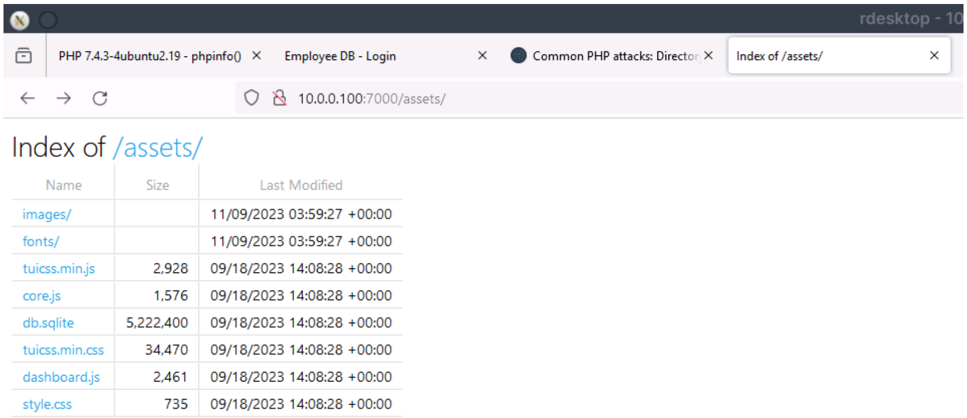
It is somewhat likely that a malicious actor exploits this vulnerability.



```
┌──(root㉿us-newengland-t6-vdi-kali02)-[~]
└─# gobuster dir -e -u http://10.0.0.100:7000 -w /usr/share/wordlists/dirb/common.txt
===============================================================
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://10.0.0.100:7000
[+] Method:                  GET
[+] Threads:                 10
[+] Wordlist:                /usr/share/wordlists/dirb/common.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.6
[+] Expanded:                true
[+] Timeout:                 10s
===============================================================
Starting gobuster in directory enumeration mode
===============================================================
http://10.0.0.100:7000/assets               (Status: 301) [Size: 0] [--> http://10.0.0.100:7000/assets/]
http://10.0.0.100:7000/index.html           (Status: 200) [Size: 1467]
Progress: 4614 / 4615 (99.98%)
===============================================================
Finished
===============================================================
```

After a web application directory scan, the path /assets/ was found. This allows a remote user to view a list of files in the directory of the server.

Proof of Compromise



Index of /assets/

Name	Size	Last Modified
images/		11/09/2023 03:59:27 +00:00
fonts/		11/09/2023 03:59:27 +00:00
tuicss.min.js	2,928	09/18/2023 14:08:28 +00:00
core.js	1,576	09/18/2023 14:08:28 +00:00
db.sqlite	5,222,400	09/18/2023 14:08:28 +00:00
tuicss.min.css	34,470	09/18/2023 14:08:28 +00:00
dashboard.js	2,461	09/18/2023 14:08:28 +00:00
style.css	735	09/18/2023 14:08:28 +00:00

Impact

While the db.sqlite file was not downloadable, if any other important documents were uploaded to this directory, they would be freely readable. With directory listings in web servers, many other vulnerabilities are close to follow. For example, while we did not fully exhaust the plethora of vulnerabilities that can be explored from this foothold, some important ones directory traversal and remote file inclusion. These vulnerabilities, along with the already-existing data exfiltration vulnerability, would result in major technical and business impacts.

Exfiltration of data as well as directory traversal could reveal important information on the server, such as the accounts on the system and sensitive data leakage such as proprietary and database information. Exploitation of these vulnerabilities could result in the attacker gaining valuable information about the layout of the system and opening the system up to further attack. Business operations are also put in danger if the attacker gains this valuable information such as database information, which can include client information, private flight information, and other personally identifiable information as well as private proprietary business data.

Remediation

Do not allow for directories to be indexed by the web server (a common configuration in many web servers). Additionally, only allowing access to certain paths and not directories can mitigate this risk.

References

https://www.cisecurity.org/controls/data-protection
https://csrc.nist.gov/pubs/sp/800/44/ver2/final

Low

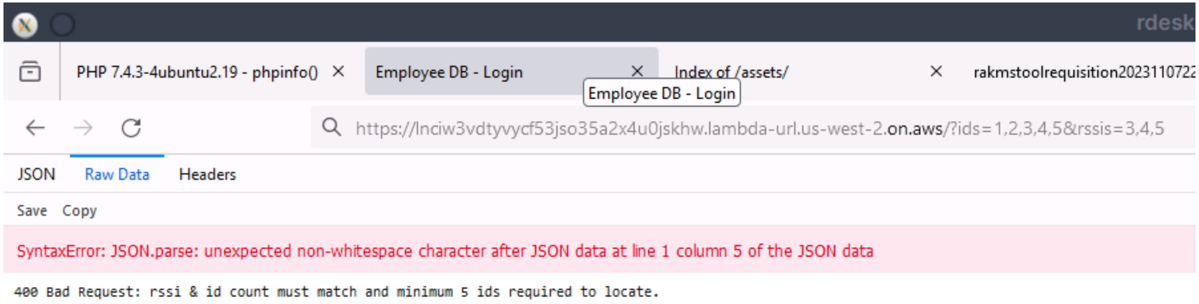
L1	Data API Publicly Available	AWS	3.0

Scope

This vulnerability affects the following AWS environment:
https://lnciw3vdtyvycf53jso35a2x4u0jskhw.lambda-url.us-west-2.on.aws/

Likelihood of Exploitation

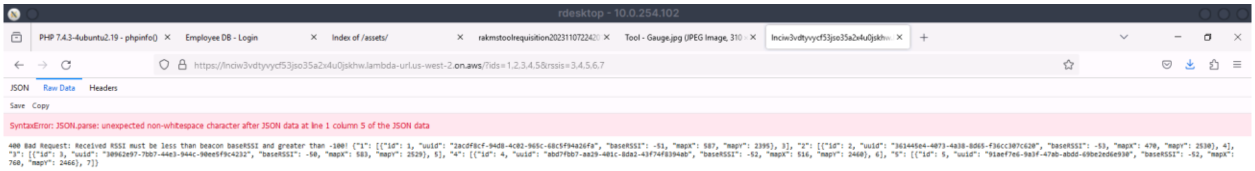
It is not very likely that this vulnerability will be exploited. The attacker would first have to locate the endpoint and then follow the helpful error messages (a security flaw!) until they could successfully and blindly form a proper JSON object to exfiltrate the data.


rdesk
PHP 7.4.3-4ubuntu2.19 - phpinfo()
Employee DB - Login
Index of /assets/
rakmstoolrequisition2023110722
Employee DB - Login
https://lnciw3vdtyvycf53jso35a2x4u0jskhw.lambda-url.us-west-2.on.aws/?ids=1,2,3,4,5&rssis=3,4,5
JSON
Raw Data
Headers
Save
Copy

SyntaxError: JSON.parse: unexpected non-whitespace character after JSON data at line 1 column 5 of the JSON data

```
400 Bad Request: rssi & id count must match and minimum 5 ids required to locate.
```

Proof of Compromise


rdesktop - 10.0.254.102
PHP 7.4.3-4ubuntu2.19 - phpinfo()
Employee DB - Login
Index of /assets/
rakmstoolrequisition202311072242
Tool - Gauge.jpg (JPEG Image, 310
lnciw3vdtyvycf53jso35a2x4u0jskhw
https://lnciw3vdtyvycf53jso35a2x4u0jskhw.lambda-url.us-west-2.on.aws/?ids=1,2,3,4,5&rssis=3,4,5,6,7
JSON
Raw Data
Headers
Save
Copy

SyntaxError: JSON.parse: unexpected non-whitespace character after JSON data at line 1 column 5 of the JSON data

```
400 Bad Request: Received RSSI must be less than beacon baseRSSI and greater than -100! {"1": [{"id": 1, "uuid": "2acdf8cf-94d8-4c02-965c-68c5f94a26fa", "baseRSSI": -51, "mapX": 587, "mapY": 2395}, 3], "2": [{"id": 2, "uuid": "361445e4-4073-4a38-8d65-f36cc307c620", "baseRSSI": -53, "mapX": 470, "mapY": 2530}, 4],
"3": [{"id": 3, "uuid": "30962e97-7bb7-44e3-944c-90ee5f9c4232", "baseRSSI": -50, "mapX": 583, "mapY": 2529}, 5], "4": [{"id": 4, "uuid": "abd7fbb7-aa29-401c-8da2-43f74f8394ab", "baseRSSI": -52, "mapX": 516, "mapY": 2460}, 6], "5": [{"id": 5, "uuid": "91aef7e6-9a3f-47ab-abdd-69be2ed6e930", "baseRSSI": -52, "mapX":
760, "mapY": 2466}, 7]}
```

Impact

This has low technical and business impact. It is not completely clear what this data may represent, and it does not seem to be very useful to an attacker. However, allowing any data to be unnecessarily accessed could be a potential security flaw.

Remediation

Restrict access to this API to only authorized users.

References

https://csrc.nist.gov/pubs/sp/800/44/ver2/final
https://www.cisecurity.org/controls/application-software-security

L2	Employee Database Admin Curlable	Employee Database (10.0.0.43)	2.0

Scope

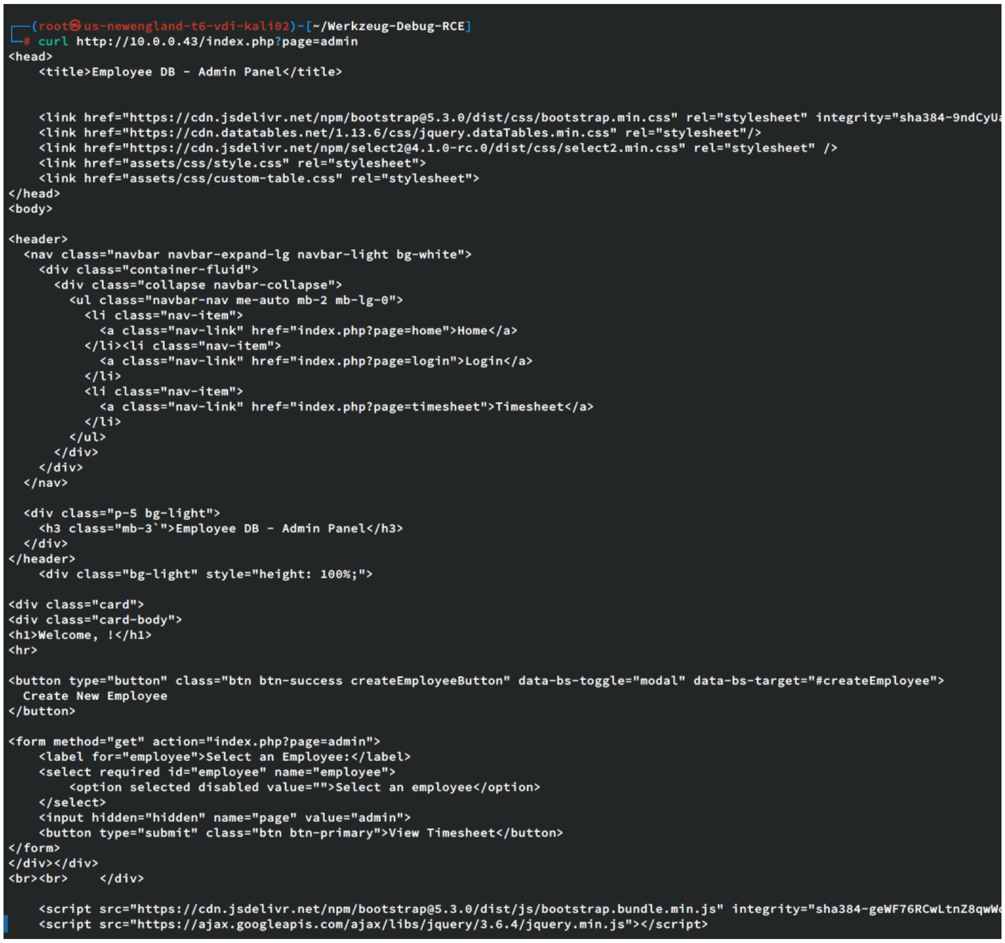
This vulnerability affects the Employee Database at 10.0.0.43.

Likelihood of Exploitation

Upon initial examination, it does not seem to be very likely that this vulnerability would be exploited. However, to an attacker with more resources and time, it is certainly more likely.

While performing routine reconnaissance, it was discovered that replacing the query string in index.php with ?page=admin instead of ?page=login, a new page was found. This was only able to be seen through cURL, and not through a browser. It is certainly possible that, with proper browser configuration, this page could be seen on a browser as well, after which an attack would be trivial.

Proof of Compromise



```
┌──(root㉿us-newengland-t6-vdi-kali02)-[~/Werkzeug-Debug-RCE]
└─# curl http://10.0.0.43/index.php?page=admin
<head>
    <title>Employee DB - Admin Panel</title>


    <link href="https://cdn.jsdelivr.net/npm/bootstrap@5.3.0/dist/css/bootstrap.min.css" rel="stylesheet" integrity="sha384-9ndCyU
    <link href="https://cdn.datatables.net/1.13.6/css/jquery.dataTables.min.css" rel="stylesheet"/>
    <link href="https://cdn.jsdelivr.net/npm/select2@4.1.0-rc.0/dist/css/select2.min.css" rel="stylesheet" />
    <link href="assets/css/style.css" rel="stylesheet">
    <link href="assets/css/custom-table.css" rel="stylesheet">
</head>
<body>

<header>
  <nav class="navbar navbar-expand-lg navbar-light bg-white">
    <div class="container-fluid">
      <div class="collapse navbar-collapse">
        <ul class="navbar-nav me-auto mb-2 mb-lg-0">
          <li class="nav-item">
            <a class="nav-link" href="index.php?page=home">Home</a>
          </li><li class="nav-item">
            <a class="nav-link" href="index.php?page=login">Login</a>
          </li>
          <li class="nav-item">
            <a class="nav-link" href="index.php?page=timesheet">Timesheet</a>
          </li>
        </ul>
      </div>
    </div>
  </nav>

  <div class="p-5 bg-light">
    <h3 class="mb-3`">Employee DB - Admin Panel</h3>
  </div>
</header>
    <div class="bg-light" style="height: 100%;">

<div class="card">
<div class="card-body">
<h1>Welcome, !</h1>
<hr>

<button type="button" class="btn btn-success createEmployeeButton" data-bs-toggle="modal" data-bs-target="#createEmployee">
  Create New Employee
</button>

<form method="get" action="index.php?page=admin">
    <label for="employee">Select an Employee:</label>
    <select required id="employee" name="employee">
        <option selected disabled value="">Select an employee</option>
    </select>
    <input hidden="hidden" name="page" value="admin">
    <button type="submit" class="btn btn-primary">View Timesheet</button>
</form>
</div></div>
<br><br>    </div>

    <script src="https://cdn.jsdelivr.net/npm/bootstrap@5.3.0/dist/js/bootstrap.bundle.min.js" integrity="sha384-geWF76RCwLtnZ8qwW
    <script src="https://ajax.googleapis.com/ajax/libs/jquery/3.6.4/jquery.min.js"></script>
```

Impact

It is not recommended to expose an admin portal, even if only through cURL. In the case that any important data, such as recent admin updates to the system, were written in this document, an attacker would be able to read it. If an attacker was able to further exploit this system by maintaining an interactive connection to this page, the business and technological impacts would be large. The attacker would have trivial access to the employee database, and could seemingly modify the timesheet, employee data, and even add their own employee to act as a back door to access the system later.

Remediation

Ensure that this system has proper access control so that only those with authorized credentials are able to view this page.

References

https://csrc.nist.gov/projects/access-control-policy-and-implementation-guides
https://csrc.nist.gov/pubs/sp/800/53/r5/upd1/final

Informational

I1	EternalBlue – CVE-2017-0144	SkyControl-01 (10.0.0.5:445)	0.0

Scope

The affected system is the domain controller SkyControl-01, located at 10.0.0.5, on port 445.

Likelihood of Exploitation

This exploit is fairly likely once a user has access to the corporate network. EternalBlue is a remarkably well-known exploit, and since the vulnerable protocol (SMBv1) is discoverable via simple port scans.

Proof of Compromise

Although the server is vulnerable, this exploit was not needed, due to the discovery of Critical Vulnerability C1. Because the server was compromisable through a different route, this exploit is redundant (although it should still be remediated!)

Impact

See impact for Critical Vulnerability C1.

Remediation

See remediation for Critical Vulnerability C1.

References

https://en.wikipedia.org/wiki/EternalBlue

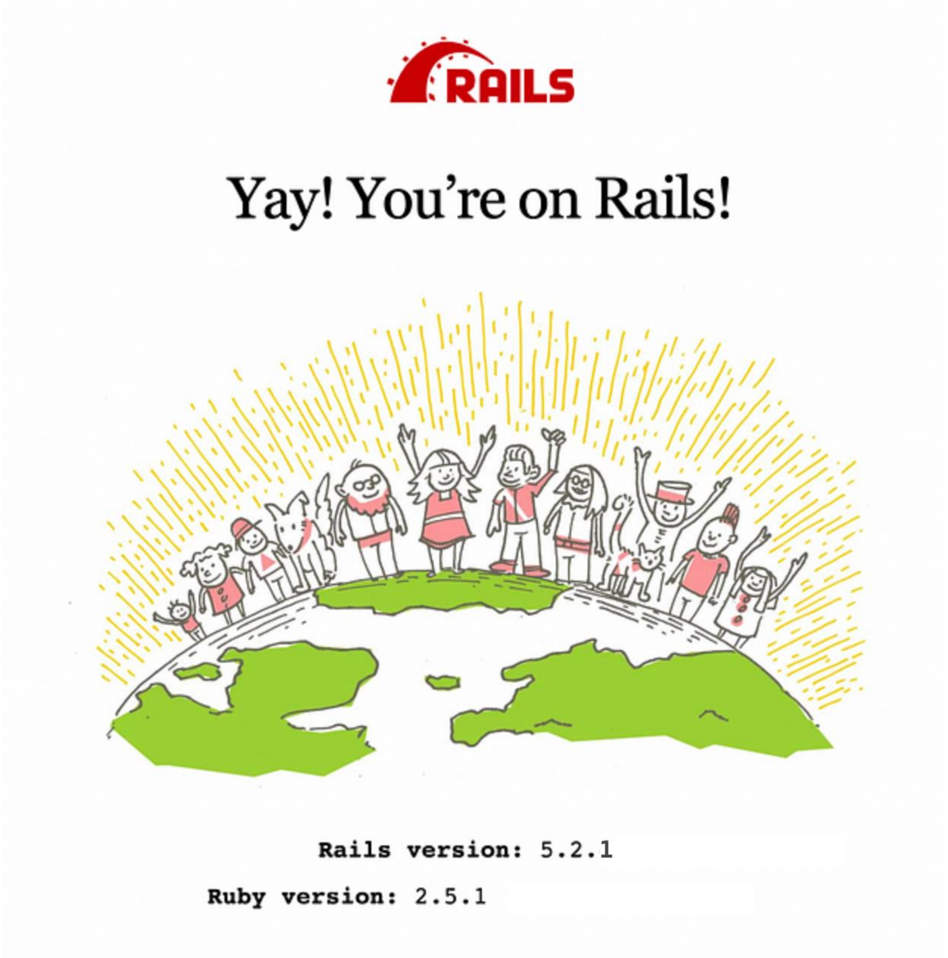
I2	DoubleTap Rails Vulnerability	TramOps (10.0.200.100:3000)	0.0

Scope

The affected system is the TramOps server at 10.0.200.100 on port 3000.

Likelihood of Exploitation

This server is correctly configured not to present the development environment, and as such is not currently vulnerable. However, if at any point the server were to be set to development mode, an easy mistake to make when testing changes, the application would become vulnerable. Additionally, the vulnerability could be planned for in advance, since the default HTTP response from the server displays the Rails and Ruby versions prominently (pictured below).



Yay! You're on Rails!

```
Rails version: 5.2.1
Ruby version: 2.5.1
```

Since the version is so clearly displayed, it is relatively trivial to google vulnerabilities for this version, leading to a very powerful CVE that allows for remote exploitation. A Metasploit module for this vulnerability is also available, further lowering the barrier to compromise.

Proof of Compromise

Since the server was not vulnerable to this attack as configured, it was not compromised.

Impact

Were the server to be compromised, an attacker would presumably gain control over the operation of the tram system, significantly affecting user experience and possibly endangering any users currently on the tram.

Remediation

Upgrading to more recent versions of Ruby and Rails would quickly remediate this vulnerability. In addition, removing the default Rails splash page would limit the amount of information available to would-be attackers.

References

https://nvd.nist.gov/vuln/detail/CVE-2019-5420

Appendix

Sources

1. http://www.pentest-standard.org/index.php/Main_Page
2. https://www.first.org/cvss/v3.0/specification-document