

DATA SECURITY ASSESSMENT REPORT

-Group 26

EXECUTIVE SUMMARY

The AWS Cloud environment's security mechanisms were the primary focus of the data security assessment. Strong encryption standards for data in transit and at rest were found in the assessment, along with clearly defined access rules that adhered to the least privilege concept. Furthermore, efficient recording and monitoring systems that improved activity visibility were noted. The security posture is further strengthened by compliance with standards and the existence of a documented incident response plan. Enhancing security documentation, putting continuous monitoring into practice, and doing recurring security assessments are among the recommendations. All things considered; the AWS cloud ecosystem shows a solid dedication to data protection.

SUMMARY OF FINDINGS

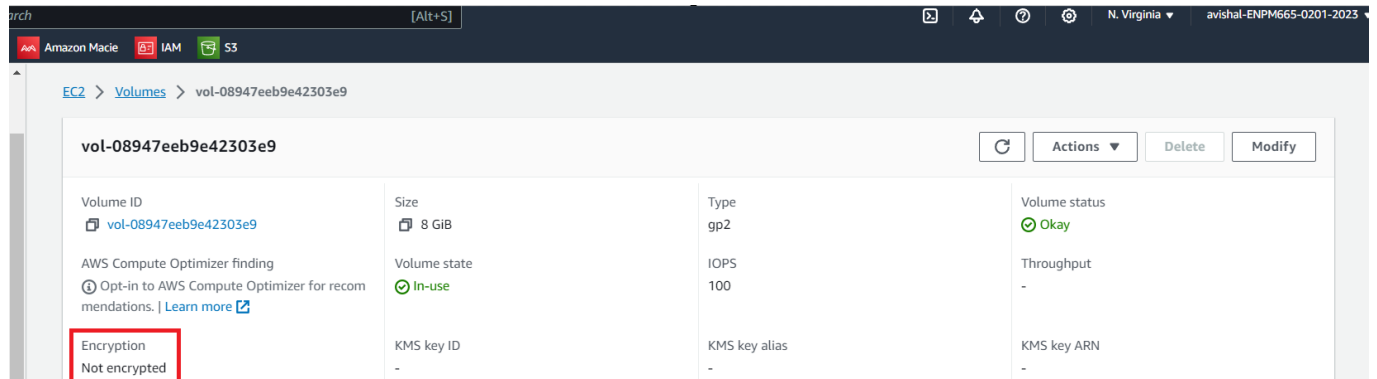
AWS Resource	Security Misconfiguration/Vulnerability	Severity
Volumes	EBS volume is unencrypted.	Medium
RDS	RDS Instance does not have enhanced monitoring enabled. RDS Instance deletion protection is not enabled. RDS Instance does not have multi-AZ enabled. Storage autoscaling disabled for RDS instance. No Password policies are used to enforce password complexity requirement.	Medium
S3	Potential secret found in S3 buckets output	Critical
	S3 User has no type of MFA enabled. S3 bucket MFA Delete is not enabled for medcirclepatientdata1. S3 buckets do not have KMS Encryption enabled. S3 bucket does not have a secure transport policy. S3 bucket medcirclepatientdata1 has versioning disabled. S3 bucket medcirclepatientdata1 has server logging access disabled. S3 bucket has CloudFormation termination protection disabled.	Medium
	S3 buckets have object lock disabled for medcirclepatientdata1. S3 User has the inline policy bucket-access attached.	Low
Encryption	AWS CloudTrail is not enabled in all regions.	High
	The storage for the Amazon RDS instances is not encrypted	Medium

VOLUMES

EBS volume is unencrypted.

Description: The default encryption for Amazon Elastic Block Store (EBS) volumes is not activated in the AWS account.

Severity: Medium



Potential Impact:

Data encryption at rest prevents data visibility in the event of its unauthorized access or theft. Higher risk of not protecting sensitive information which is at rest and could lead to compliance and security risks.

Remediation Recommendations:




Encrypt all EBS volumes and enable default encryption for EBS volumes in the AWS account. This will ensure that all new EBS volumes are encrypted by default.

RDS

RDS Instance deletion protection is not enabled.

Description:

Severity: Medium

Configuration	Instance class
DB instance ID midterm-group26-avishal-infrastructure-dbinstance-wlh7fvu1449j	Instance class db.t2.micro
Engine version 8.0.33	vCPU 1
DB name MedCircleDB	RAM 1 GB
License model General Public License	Availability
Option groups default:mysql-8-0  In sync	Master username doctorenmp665
Amazon Resource Name (ARN)  arn:aws:rds:us-east-1:964706929724:db:midterm-group26-avishal-infrastructure-dbinstance-wlh7fvu1449j	Master password *****
Resource ID db-TGCCTGHNEBYACNXQDBWN6NH6TY	IAM DB authentication Not enabled
Created time October 27, 2023, 18:31 (UTC-04:00)	Multi-AZ No
DB instance parameter group default.mysql8.0  In sync	Secondary Zone -
Deletion protection Disabled	

Potential Impact:

An increased chance of inadvertent deletion is one possible consequence of not having deletion protection enabled for the RDS instance. There is a greater chance that the RDS instance may be inadvertently destroyed, which could result in data loss and possible outages for applications that depend on the database.



Remediation Recommendations:

Activate deletion protection for the RDS instance to prevent accidental deletion, review the settings of RDS instances to ensure deletion protection remains enabled.

RDS Instance does not have multi-AZ enabled.

Description: Multi-AZ (Availability Zone) deployment is not enabled for the Amazon RDS instance.

Severity: Medium

Instance	
Configuration	Instance class
DB instance ID	Instance class
midterm-group26-avishal-infrastructure-dbinstance-wlh7fvu1449j	db.t2.micro
Engine version	vCPU
8.0.33	1
DB name	RAM
MedCircleDB	1 GB
License model	Availability
General Public License	Master username
Option groups	doctorenmp665
default:mysql-8-0  In sync	Master password
Amazon Resource Name (ARN)	*****
 arn:aws:rds:us-east-1:964706929724:db:midterm-group26-avishal-infrastructure-dbinstance-wlh7fvu1449j	IAM DB authentication
Resource ID	Not enabled
db-TGCCTGHNEBYACNXQDBWN6NH6TY	Multi-AZ
Created time	No
October 27, 2023, 18:31 (UTC-04:00)	Secondary Zone
	-

Potential Impact:

If the RDS instance's Multi-AZ deployment is not enabled, there may be a greater chance of downtime in the case of an Availability Zone failure. There would be no automatic failover to a standby instance in a separate Availability Zone in the absence of Multi-AZ, which could cause service disruption and application outages.



Remediation Recommendations:

Activate Multi-AZ deployment for the RDS instance to benefit from automatic failover to a standby instance in a different Availability Zone.

Storage autoscaling disabled for RDS instance.

Description: Storage autoscaling is disabled for the Amazon RDS instance.

Severity: Medium

Instance		
Configuration	Instance class	Storage
DB instance ID midterm-group26-avishal-infrastructure-dbinstance-wlh7fvu1449j	Instance class db.t2.micro	Encryption Not enabled
Engine version 8.0.33	vCPU 1	Storage type General Purpose SSD (gp2)
DB name MedCircleDB	RAM 1 GB	Storage 20 GiB
License model General Public License	Availability	Provisioned IOPS -
Option groups default:mysql-8-0  In sync	Master username doctorenmp665	Storage throughput -
Amazon Resource Name (ARN)  arn:aws:rds:us-east-1:964706929724:db:midterm-group26-avishal-infrastructure-dbinstance-wlh7fvu1449j	Master password *****	Storage autoscaling Disabled
	IAM DB authentication Not enabled	Storage file system configuration Current
	Multi-AZ	

Potential Impact:

If the database grows larger than the allotted storage capacity, one possible consequence of not having storage autoscaling enabled for the RDS instance is that storage may run out.

Data loss, service disruptions, and the requirement for manual intervention to expand storage capacity might result from this.

Remediation Recommendations:

Activate storage autoscaling for the RDS instance to allow for automatic adjustment of storage capacity based on usage.

RDS Instance does not have enhanced monitoring enabled.

Description: The Amazon RDS (Relational Database Service) instance does not have enhanced monitoring enabled.

Severity: Medium

The screenshot displays the AWS Management Console for an Amazon RDS instance. The instance name is 'midterm-group26-avishal-infrastructure-dbinstance-wlh7fvu1449j'. The 'Monitoring' tab is active, showing a summary of the instance's status (Available), CPU usage (5.42%), and connections (0). A notification banner indicates that a new monitoring view is available, which includes Performance Insights and CloudWatch metrics. A dropdown menu is open, showing options for 'Enhanced monitoring', 'OS process list', and 'Performance Insights'. The 'Enhanced monitoring' option is highlighted with a red box.

Potential Impact:

A smaller monitoring interval results in more frequent reporting of OS metrics. Lowered awareness of operational insights and performance metrics.

Remediation Recommendations:

Create an IAM role and enable enhanced monitoring.

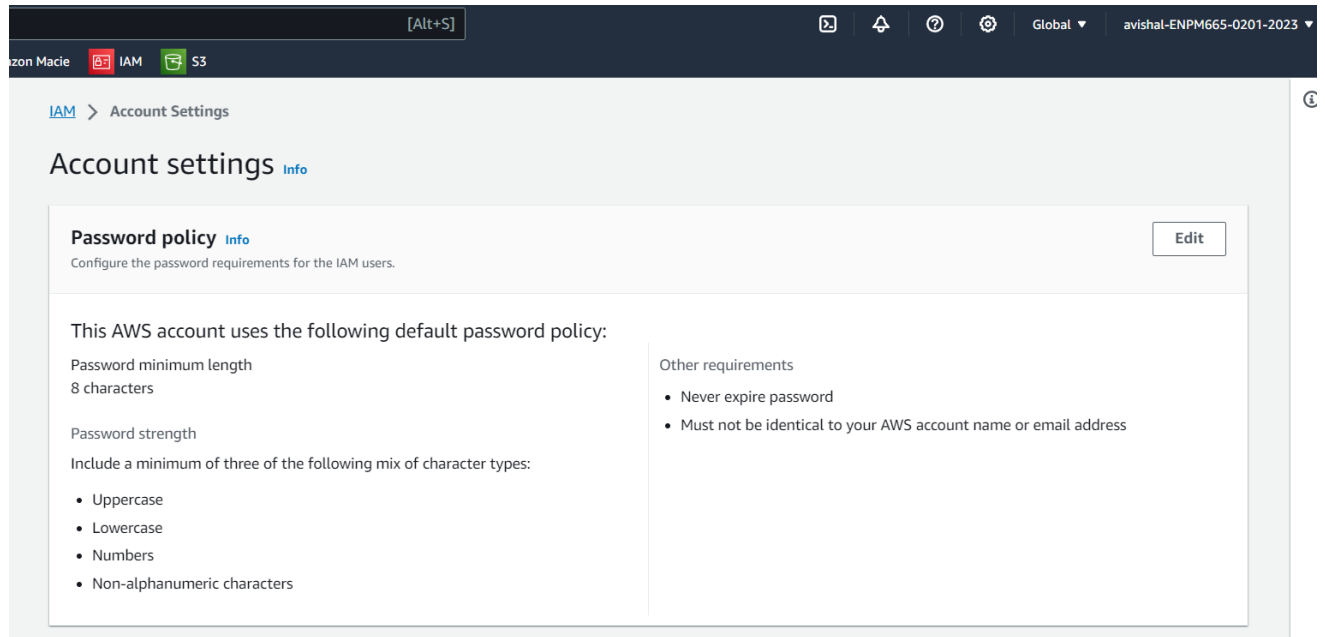
No Password policies are used to enforce password complexity requirement.

Description: The AWS account does not have a password policy enforced. Specifically, passwords do not expire, and no password policies are in place to enforce complexity requirements.

Severity: Medium

Potential Impact:

Includes increased security risks due to the absence of controls over password expiration and complexity, Increased Vulnerability to Brute Force Attacks, Higher Risk of Unauthorized Access, Increased Support Overhead.



Remediation Recommendations:

Implement password policies, enforce password expiration, regularly review and update policies. Set the rules to enhance the complexity of the password.

S3 BUCKET

Potential secret found in S3 buckets output.

Description: Potential secret found in S3 buckets output

Severity: Critical

Outputs (4)				
<input type="text" value="Search outputs"/>				
Key	Value	Description	Export name	
AccessKeyID	AKIAVARV57PEJN5CELGF	-	-	
BucketName	medcirclepatientdata1-344784239560	-	-	
SecretAccessKey	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	-	-	
User	midterm-group26-smehta23-s3-S3User-1LRYBUX0N7YV5	-	-	

Potential Impact:

Patient data can be seriously at risk of security breaches if secret access keys are left exposed in the output of an S3 bucket or any other resource.

If these keys are acquired by unauthorized parties, it could result in data breaches, malicious access to patient information, and possible violations of healthcare data protection laws, all of which could have catastrophic financial and legal repercussions for the healthcare organization.

Remediation:

Implement automated detective control to scan accounts for passwords and secrets. Use secrets manager service to store and retrieve passwords and secrets.

S3 User has no type of MFA enabled.

Description: S3 User has no type of MFA enabled

Severity: Medium

Patient1

Info

Delete

Summary

ARN
arn:aws:iam::344784239560:user/Patient1

Console access
Disabled

Access key 1
[Create access key](#)

Created
October 26, 2023, 21:06 (UTC-04:00)

Last console sign-in
-

Permissions

Groups

Tags

Security credentials

Access Advisor

Console sign-in

Enable console access

Console sign-in link
<https://shikha1149.signin.aws.amazon.com/console>

Console password
Not enabled

Multi-factor authentication (MFA) (0)

Use MFA to increase the security of your AWS environment. Signing in with MFA requires an authentication code from an MFA device. Each user can have a maximum of 8 MFA devices assigned. [Learn more](#)

Remove

Resync

Assign MFA device

Device type

Identifier

Certifications

Created on

No MFA devices. Assign an MFA device to improve the security of your AWS environment

Assign MFA device

Potential Impact:

Patient accounts are more susceptible to illegal access without MFA, endangering the confidentiality and security of their medical records.

Sensitive health information may be revealed as a result, which could violate HIPAA and other laws protecting healthcare data and have negative legal and financial repercussions.

Remediation:

Enable hardware MFA device for an IAM user from the AWS Management Console; the command line; or the IAM API.

S3 bucket MFA Delete is not enabled for medcirclepatientdata1.

Description: S3 bucket MFA Delete is not enabled for medcirclepatientdata1

Severity: Medium

Potential Impact:


Patient data may be more vulnerable to illegal data deletion or tampering if Multi-Factor Authentication (MFA) is disabled.

This could jeopardize the accuracy and integrity of patient records. In addition to possible legal repercussions, this may result in privacy violations, compliance infractions, and harm to the healthcare organization's brand.

medcirclepatientdata1-344784239560 [Info](#)

[Objects](#) [Properties](#) [Permissions](#) [Metrics](#) [Management](#) [Access Points](#)

Bucket overview

AWS Region US East (N. Virginia) us-east-1	Amazon Resource Name (ARN)  arn:aws:s3:::medcirclepatientdata1-344784239560	Creation date October 26, 2023, 21:01:24 (UTC-04:00)
---	---	---

Bucket Versioning [Edit](#)

Versioning is a means of keeping multiple variants of an object in the same bucket. You can use versioning to preserve, retrieve, and restore every version of every object stored in your Amazon S3 bucket. With versioning, you can easily recover from both unintended user actions and application failures. [Learn more](#)

Bucket Versioning

Disabled

Multi-factor authentication (MFA) delete

An additional layer of security that requires multi-factor authentication for changing Bucket Versioning settings and permanently deleting object versions. To modify MFA delete settings, use the AWS CLI, AWS SDK, or the Amazon S3 REST API. [Learn more](#)

Disabled

Remediation:

Adding MFA delete to an S3 bucket, requires additional authentication when you change the version state of your bucket, or you delete an object version adding another layer of security in the event your security credentials are compromised or unauthorized access is granted.

S3 buckets do not have KMS Encryption enabled.

Description: S3 buckets do not have KMS Encryption enabled

Severity: Medium

Default encryption [Info](#) [Edit](#)

Server-side encryption is automatically applied to new objects stored in this bucket.

Encryption type [Info](#)

Server-side encryption with Amazon S3 managed keys (SSE-S3)

Bucket Key

When KMS encryption is used to encrypt new objects in this bucket, the bucket key reduces encryption costs by lowering calls to AWS KMS. [Learn more](#)

Disabled

Potential Impact:

Patient data that is not encrypted using S3 KMS (Key Management Service) may be more vulnerable to illegal access, data leaks, and privacy violations. This exposes private patient data and could lead to legal troubles for the healthcare provider as well as regulatory violations.

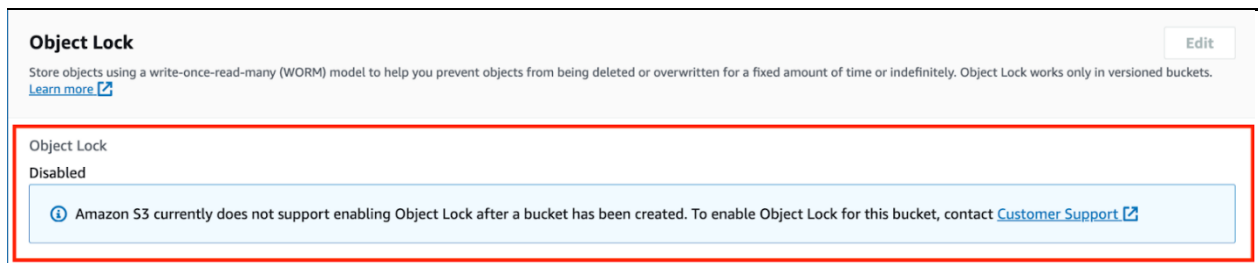
Remediation:

Ensure that S3 buckets have encryption at rest enabled using KMS.

S3 buckets have object lock disabled for medcirclepatientdata1.

Description: S3 buckets have object lock disabled for medcirclepatientdata1

Severity: Low



Potential Impact:

Disabling Object Lock for patient data in an Amazon S3 bucket may increase the chance that data will be deleted unintentionally or on purpose, endangering data integrity and increasing the possibility of unauthorized changes. Without Object Lock, there is less chance that patient data will be shielded from alteration or deletion, which could result in data loss, security breaches, and problems with complying with regulations.

Remediation:

Ensure that your Amazon S3 buckets have Object Lock feature enabled to prevent the objects they store from being deleted.

S3 bucket medcirclepatientdata1 has versioning disabled.

Description: S3 bucket medcirclepatientdata1 has versioning disabled

Severity: Medium


Potential Impact:

It eliminates the option to keep older iterations of an object. There is no way to restore earlier iterations of the data in the event of deletion or unauthorized changes, which could result in data loss, make it more difficult to track changes, and make the data more vulnerable to breaches or unauthorized alterations.


medcirclepatientdata1-344784239560 [Info](#)

Objects **Properties** Permissions Metrics Management Access Points

Bucket overview

AWS Region US East (N. Virginia) us-east-1	Amazon Resource Name (ARN)  arn:aws:s3:::medcirclepatientdata1-344784239560	Creation date October 26, 2023, 21:01:24 (UTC-04:00)
---	---	---

Bucket Versioning [Edit](#)

Versioning is a means of keeping multiple variants of an object in the same bucket. You can use versioning to preserve, retrieve, and restore every version of every object stored in your Amazon S3 bucket. With versioning, you can easily recover from both unintended user actions and application failures. [Learn more](#) 

Bucket Versioning
Disabled

Remediation:


Configure versioning using the Amazon console or API for buckets with sensitive information that is changing frequently; and backup may not be enough to capture all the changes.



S3 bucket does not have a secure transport policy.

Description: S3 bucket medcirclepatientdata1 has no bucket policy, thus allowing http traffic. S3 bucket does not have a secure transport policy.

Severity: Medium

Bucket policy [Edit](#) [Delete](#)

The bucket policy, written in JSON, provides access to the objects stored in the bucket. Bucket policies don't apply to objects owned by other accounts. [Learn more](#) 

 **Public access is blocked because Block Public Access settings are turned on for this bucket**
To determine which settings are turned on, check your Block Public Access settings for this bucket. [Learn more about using Amazon S3 Block Public Access](#) 

Potential Impact:

Without a bucket policy, access control rules for patient data stored in an Amazon S3 bucket are not established, which could result in unrestricted and public access to the information. This lack of access controls puts patient data security and privacy at risk by exposing data, allowing unauthorized access, and raising the possibility of data breaches.

Remediation:

Ensure that S3 buckets have encryption in transit enabled.

S3 bucket has CloudFormation termination protection disabled.

Description: S3 bucket has CloudFormation termination protection disabled

Severity: Medium

Stack ID arn:aws:cloudformation:us-east-1:344784239560:stack/midterm-group26-smehta23-s3/574b5350-7464-11ee-aff0-12869112c9e5	Description Create an S3 bucket and IAM user with access to that bucket.
Status ✔ CREATE_COMPLETE	Status reason -
Root stack -	Parent stack -
Created time 2023-10-26 21:01:20 UTC-0400	Deleted time -
Updated time -	
Drift status ⊖ NOT_CHECKED	Last drift check time -
Termination protection Deactivated	IAM role -

Potential Impact:

Disabling termination protection in AWS CloudFormation for resources holding patient data may make it more likely that vital infrastructure will be unintentionally or maliciously deleted. This could result in the loss of patient data and interfere with the provision of healthcare services, which would affect data availability and the organization's capacity to adhere to compliance and data protection regulations.

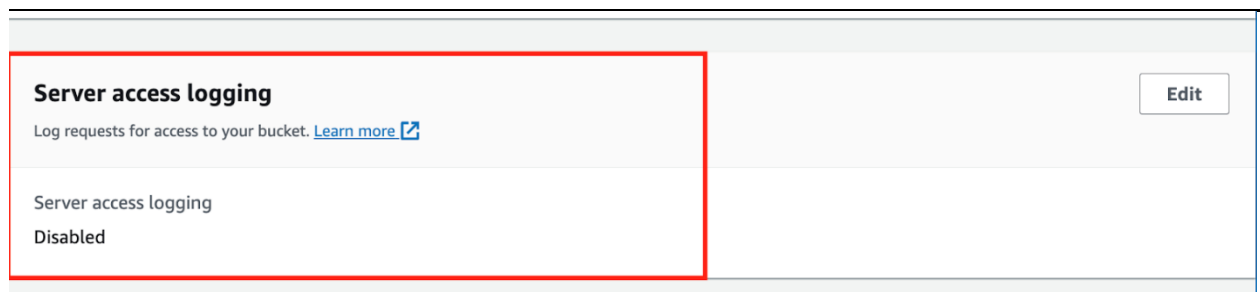
Remediation:

Ensure termination protection is enabled for the CloudFormation stacks.

S3 bucket medcirclepatientdata1 has server logging access disabled.

Description: S3 bucket medcirclepatientdata1 has server logging access disabled

Severity: Medium



Potential Impact:

When server logging access to patient data is disabled in a cloud environment, no record of who accessed the data, when, or from where is kept. Maintaining data security and compliance with patient data protection regulations may become more challenging due to this lack of visibility, which can also hinder auditing, monitoring, and investigations in the event of unauthorized access or breaches.

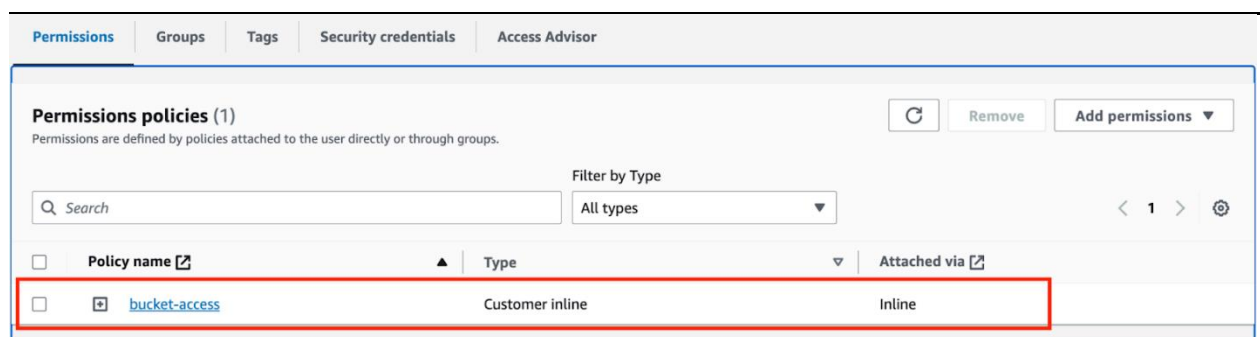
Remediation:

Ensure that S3 buckets have Logging enabled. CloudTrail data events can be used in place of S3 bucket logging. If that is the case, this finding can be considered a false positive.

S3 User has the inline policy bucket-access attached.

Description: S3 User has the inline policy bucket-access attached

Severity: Low



Potential Impact:

An S3 bucket with an inline policy attached that allows for excessive access can put patient data at serious risk of security breaches. These policies could unintentionally give unauthorized users extensive access to the data, which could lead to privacy violations and data breaches.

Remediation:



Remove any policy attached directly to the user. Use groups or roles instead.

ENCRYPTION

RDS instances storage is not encrypted.

Description: The storage for the Amazon RDS instances is not encrypted.

Severity: Medium

Instance		
Configuration	Instance class	Storage
DB instance ID midterm-group26-avishal-infrastructure-dbinstance-wlh7fvu1449j	Instance class db.t2.micro	Encryption Not enabled
Engine version 8.0.33	vCPU 1	Storage type General Purpose SSD (gp2)
DB name MedCircleDB	RAM 1 GB	Storage 20 GiB
License model General Public License	Availability	Provisioned IOPS -
Option groups default:mysql-8-0  In sync	Master username doctorenmp665	Storage throughput -
Amazon Resource Name (ARN)  arn:aws:rds:us-east-1:964706929724:db:midterm-group26-avishal-infrastructure-dbinstance-wlh7fvu1449j	Master password *****	Storage autoscaling Disabled
	IAM DB authentication Not enabled	Storage file system configuration Current
	Multi-AZ	

Potential Impact:

The possibility of data exposure and a failure to adhere to security standards are two possible effects of not having storage encryption enabled for RDS instances. If the underlying storage medium is breached, unencrypted data that is at rest may be exposed to unwanted access and possible data breaches.

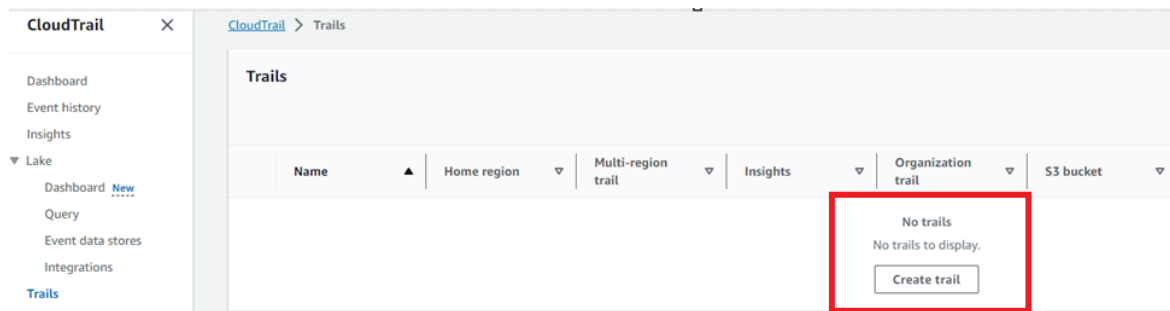
Remediation Recommendations:

Enable storage encryption, Select the appropriate encryption method, either using AWS-managed keys or customer-managed keys, based on the security and compliance requirements.

CloudTrail is not enabled in all the regions.

Description: AWS CloudTrail is not enabled in all regions.

Severity: High



Potential Impact:

Inadequate CloudTrail activation across all regions may result in restricted access to and auditability of AWS account activity. The absence of CloudTrail coverage across all regions may result in the loss of important event data, impeding efforts related to incident response, forensics, and compliance.

Remediation Recommendations:

Activate CloudTrail and review existing CloudTrail trails to ensure they are configured to record events in all necessary regions.

