ENPM695-0301

Group 13

Achuth Chandra Moonnamkuttiyil (120311482)

Srikanth Parvathala (119351192)

Subramanian Venkatachalam (120410208)

Midterm project Prowler report summary

We used **Amazon Inspector** and the third-party tool **Prowler** for finding vulnerabilities.

We've listed them as critical, high, medium and low-level vulnerabilities based on the severity ratings that we got from prowler.

Critical Severity Vulnerabilities:

- **MFA is not enabled** for root account.
- **Potential secret found in Stack** midterm-group13-subvenk-s3bucket-inclass Outputs.

High Severity Vulnerabilities:

- **Block Public Access is not configured** for the account.
- **No CloudTrail trails enabled**, and logging were found.
- AWS policy AdministratorAccess is attached and allows '*:*' administrative privileges.
- Security group PublicSG (sg-0c956812f9af549d2) has **SSH port 22 open to the Internet**.
- Security group midterm-group13-subvenk-inclass-InstanceSecurityGroup-13P51V0PN874A (sg-0afcf72a302a9e572) has **SSH port 22 open to the Internet**.
- Athena WorkGroup primary does not encrypt the query results.
- Default Security Group (sg-01d7496d880a5ded9) rules **allow traffic from everywhere.**

Medium Severity Vulnerabilities:

- **EC2 Instance** i-09283702134c21f16 has a **Public IP**: 52.203.74.48 ().
- **AWS Organizations is not in-use** for this AWS Account.
- **EBS Default Encryption is not activated**.
- **Root volume is not encrypted.**
- EC2 Instance i-09283702134c21f16 has **IMDSv2 disabled** or not required.
- Glue data catalog connection **password is not encrypted**.
- Glue data catalog settings have **metadata encryption disabled**.
- **GuardDuty is not enabled.**
- User midterm-group13-subvenk-s3bucket-inclass-S3User-4QDKSUUTU28X does **not have any type of MFA enabled.**
- User Patient1, Patient2, Patient3, Patient4, Patient5 and Patient6 users **do not have any type of MFA enabled.**
- **AWS Inspector is not enabled**.
- **RDS Instance** midterm-group13-subvenk-inclass-dbinstance-m95ne5hwgiet **deletion protection is not enabled.**
- **RDS Instance** midterm-group13-subvenk-inclass-dbinstance-m95ne5hwgiet **does not have CloudWatch Logs enabled.**
- **RDS Instance** midterm-group13-subvenk-inclass-dbinstance-m95ne5hwgiet **is not encrypted.**
- **S3 Bucket** cf-templates-1l2alfu2wb361-us-east-1 has **MFA Delete disabled.**
- **S3 Bucket** medcirclepatientdata1-666477007806 has **MFA Delete disabled.**
- **Server-Side Encryption is not configured with kms** for S3 Bucket cf-templates-1l2alfu2wb361-us-east-1.
- **Server-Side Encryption is not configured with kms for S3 Bucket** medcirclepatientdata1-
- **S3 Bucket** cf-templates-1l2alfu2wb361-us-east-1 has **versioning disabled.**
- **S3 Bucket** medcirclepatientdata1-666477007806 has **versioning disabled.**
- **S3 Bucket** cf-templates-1l2alfu2wb361-us-east-1 **does not have a bucket policy; thus, it allows HTTP requests.**

- **S3 Bucket** medcirclepatientdata1-666477007806 **does not have a bucket policy; thus, it allows HTTP requests.**
- **S3 Bucket** cf-templates-1l2alfu2wb361-us-east-1 has **server access logging disabled.**
- **AWS Security Hub is not enabled.**
- **CloudFormation** midterm-group13-subvenk-users-inclass **has termination protection disabled.**
- **No CloudWatch log groups found with metric filters or alarms associated.**
- **VPC** vpc-0ab29ea1e84cb6007 **does not have Network Firewall enabled.**
- **VPC** vpc-0195acf48d9737361 **does not have Network Firewall enabled.**
- **AWS Config recorder** 666477007806 **is disabled.**
- **DRS is not enabled for this region.**
- **EC2 Instance** i-09283702134c21f16 **not associated with an Instance Profile Role.**
- **Password policy cannot be found.**
- **Network ACL** acl-0a1fb900d96b16356 has **every port open to the Internet.**
- **Network ACL** acl-0a1fb900d96b16356 has **Microsoft RDP port 3389 open to the Internet.**
- **Network ACL** acl-0a1fb900d96b16356 has **SSH port 22 open to the Internet.**
- **No SSM Incidents replication set exists.**
- **EBS Snapshot** vol-08f20e6142e7a6bc7 **is unencrypted.**
- **VPC** vpc-0ab29ea1e84cb6007 **Flow logs are disabled.**
- **VPC subnet** subnet-0cae7f359815eb936 **assigns public IP by default.**
- **GuardDuty detector** 666477007806 **is not centrally managed.**

Low Severity vulnerabilities:

- **Macie is not enabled.**
- **EC2 Instance** i-09283702134c21f16 **does not have detailed monitoring enabled.**
- **IAM Access Analyzer** in account 666477007806 **is not enabled.**
- **RDS Instance** midterm-group13-subvenk-inclass-dbinstance-m95ne5hwgiet does **not have enhanced monitoring enabled.**

- **S3 Bucket** cf-templates-1l2alfu2wb361-us-east-1 **has Object Lock disabled.**
- **S3 Bucket** medcirclepatientdata1-666477007806 **has Object Lock disabled.**
- **No CloudTrail trails have a data event to record all S3 object-level API operations.**
- **SecurityAudit policy is not attached to any role.**
- **No Backup Vault exist.**
- User midterm-group13-subvenk-s3bucket-inclass-S3User-4QDKSUUTU28X has the **inline policy bucket-access attached.**
- **No Backup Plan exist**.
- **Security group PublicSG** (sg-0c956812f9af549d2) **it is not being used.**
- **Security group PrivateSG** (sg-0ffda419fc28a8f33) **it is not being used.**
- **No Resource Explorer Indexes found.**