Operational Disruption: AWS Middle East Regions Impacted by Drone Strikes Affecting Multiple Services

Tracking ID#: PCS-03-0326

Date: 03-03-2026

Disclaimer: This is a shared security advisory service; hence, it can be communicated to a single dedicated point of contact. We would highly appreciate it if you assigned them to your organisation's concerned asset/technology owner. Please use it as applicable to your environment

Date: 03-03-2026

Summary:

Amazon Web Services (AWS) is facing a major disruption in its Middle East (UAE) Region (ME-CENTRAL-1) and Middle East (Bahrain) Region (ME-SOUTH-1). This is due to physical damage caused by drone strikes during the ongoing regional conflict. In the UAE, two facilities were hit directly, affecting two of the three Availability Zones (mec1-az2 and mec1-az3). In Bahrain, a drone strike near one facility caused damage. The strikes caused structural damage, power outages, and some fires that led to water damage from suppression efforts. AWS is working with local authorities and focusing on staff safety as they recover. Power is still out in the affected zones, and recovery will take several days because of the damage. Key services like Amazon S3, Amazon DynamoDB, and Amazon EC2 are heavily affected. S3 is having many failures with data upload and download due to the two damaged Availability Zones. DynamoDB error rates are still high. EC2 instance launches are limited across the region, and existing instances in the damaged zones are down. Many related services in compute, storage, database, networking, and management are also affected. AWS is working on two recovery approaches: fixing the physical infrastructure and software fixes to restore services without full repairs. These efforts include updates to help S3 work within current limits, fixing DynamoDB tables, and network changes to restore Management Console and CLI access. The third Availability Zone (mec1-az1) in UAE is still working normally, but some services are indirectly affected because they depend on the damaged zones. AWS strongly advises customers to use their disaster recovery plans, move workloads to other AWS Regions (like US, Europe, or Asia Pacific), and update apps to avoid the affected regions. The situation in the Middle East is still unstable. AWS will provide more updates as recovery continues. The following services are currently disrupted or degraded:

- **Disrupted (25 services):** AWS Backup, CloudTrail, Compute Optimizer, Elastic Beanstalk, Fargate, IoT Core, IoT Device Defender, IoT Device Management, Lambda, License Manager, Management Console, Athena, DocumentDB, EC2, ECR, ECS, EFS, EKS, EventBridge, EventBridge Scheduler, Kinesis Data Streams, Redshift, RDS, SNS, S3.

- **Degraded (34 services):** AppConfig, Application Migration Service, Client VPN, CodeBuild, Config, Database Migration Service, Direct Connect, Elastic Disaster Recovery, Elemental, End User Messaging, Glue, KMS, NAT Gateway, Network Firewall, Private CA, Security Hub, Service Catalog, Step Functions, Systems Manager for SAP, Transit Gateway, CloudWatch, Cognito, DynamoDB, EMR Serverless, Elastic Load Balancing, EMR, FSx, Glacier, GuardDuty, OpenSearch Service, Route 53, SES, SQS, SWF.

- **Impacted (50 services):** Amplify, AppSync, Batch, Certificate Manager, Cloud Map, Cloud WAN, CloudFormation, CloudHSM, CloudShell, CodeDeploy, CodePipeline,

Control Tower, DataSync, Directory Service, Firewall Manager, IAM Identity Center, IAM Roles Anywhere, Lake Formation, Resource Explorer, Resource Groups, Resource Groups Tagging API, Secrets Manager, Security Incident Response, STS, Sign-In, Site-to-Site VPN, Storage Gateway, Systems Manager, Transfer Family, VPCE PrivateLink, Verified Access, WAF, API Gateway, ElastiCache, Inspector, Kinesis Firehose, MQ, Managed Grafana, Managed Service for Apache Flink, Managed Service for Prometheus, Managed Streaming for Apache Kafka, Neptune, SageMaker, VPC IP Address Manager, VPC Lattice, VPC, WorkSpaces, Auto Scaling, EC2 Image Builder, Reachability Analyzer.

- **Resolved (3 services):** Global Accelerator, CloudFront, Traffic Mirroring.

Target:

Applicable to all AWS customers in the Middle East regions.

Mitigation Recommendations:

- We strongly recommend that customers with workloads running in the Middle East take action now to migrate those workloads to alternate AWS Regions.
- Customers should enact their disaster recovery plans, recover from remote backups stored in other regions, and update their applications to direct traffic away from the affected regions.
- For customers requiring guidance on alternate regions, we recommend considering AWS Regions in the United States, Europe, or Asia Pacific, as appropriate for your latency and data residency requirements.

References:

https://health.aws.amazon.com/health/status