AWS Incident Analysis Report

Incident Summary  
On October 20, 2025 Amazon Web Services (AWS) detected a significant increase in error rates and elevated latencies across multiple services in the US-EAST-1 (Virginia) region. The affected services include Amazon Dynamo DB, Amazon SQS (Simple Queue Service), EC2 (elastic Compute Cloud), AWS Lambda event-source polling and other dependent services.

This outage caused global disruptions, impacting major consumer and enterprise platforms such as Snapchat, Roblox, and several financial services in the Uk. AWS began investigating at 12:11AM PDT and by 2:01AM PDT a potential root cause had been identified – an issue related to DNS resolution of the DynamoDB API endpoint in the affected region.

To restore services, AWS implemented several mitigation steps, including rate-limiting EC2 instance launches, processing backlogs, and recommending DNS cache flushing. These actions led to “significant signs of recovery” later that morning. There is no evidence to suggest that the outage was caused by a malicious attack.

# Impact Analysis

This incident has a major impact on Plymouth Retail LTD, which relies heavily on AWS infrastructure to host and manage its online retail operations. Even though our company’s primary systems may not reside in the US-EAST-1 region, disruptions can still indirectly affect global services through shared dependencies and cross-regional integrations.

**Key Impact on Plymouth Retail LTD**

1. **Customer Experience**

* Our e-commerce website may have experience downtime or slow performance, preventing customers from browsing products or placing orders.
* Failed transactions could have led to customer frustration and an increased in support requests.

1. **Revenue and Operational Disruption**

* Temporarily unavailability of EC2, SQS, or DynamoDB services could have halted order processing, leading to loss of sales and potential data synchronization issues.
* Internal processes, such as inventory tracking or order fulfillment, may have faced delays.

1. **Reputation and Risk Exposure**

* Extended downtime can negatively affect customer trust and brand reputation.
* This event also highlights Plymouth Retail LTDs dependency on a single cloud provider, revealing potential single points of failure in our infrastructure.

# Recommendations

To reduce the risk and impact of similar incidents in the future, the following measures are recommended:

1. **Implement Multi-Region Deployment and Redundancy**
   * Deploying critical systems across multiple AWS regions (or availability zones) ensures service continuity even if one region experiences an outage.
   * This strategy minimizes downtime and maintains customer access to our online store.
2. **Adopt a Hybrid or Multi-Cloud Strategy**
   * Integrating backup services with another cloud provider (e.g., Microsoft Azure or Google Cloud) provides an additional layer of resilience.
   * This reduces dependency on a single provider and helps mitigate global-scale outages in future.
3. **Establish Incident Response and Communication Protocols**
   * Creating a clear internal incident response plan and customer communication strategy ensures rapid action and transparency during outages.
   * Regular monitoring, early warning alerts, and escalation procedures can help identify issues before they severely impact operations.