Cybersecurity Incident Report

Date: March 10, 2025

Prepared by: Agbai Joseph Okwara

Affected Account: AWS Account ID: 879381240505

Incident Summary:

This report analyzes unusual activity recorded in AWS CloudTrail logs for the AWS root account (ID: 879381240505). The logs indicate multiple failed access attempts and suspicious API calls from an external IP address (178.153.40.80). Notably, Multi-Factor Authentication (MFA) was not enabled for the root user, increasing the risk of unauthorized access.

Findings:

1. **Unauthorized API Calls:**
    - Multiple API calls were attempted using root account credentials:
        - **Event Source:** sso.amazonaws.com
        - **Event Name:** DescribeRegisteredRegions
        - **Response:** AccessDenied error
        - **Timestamp:** 03:26:38 UTC & 03:31:20 UTC
        - **Event Source:** notifications.amazonaws.com
        - **Event Name:** GetFeatureOptInStatus
        - **Response:** No response elements provided
        - **Timestamp:** 03:27:26 UTC & 03:30:41 UTC
2. **Potential Unauthorized Access Indicators:**
    - API requests were made using a root account without MFA authentication.
    - Repeated requests from an unfamiliar IP address 178.153.40.80.
    - AccessDenied errors suggest an attempt to query AWS SSO configurations.
    - Session credentials were obtained from the AWS Console (sessionCredentialFromConsole: true).
3. **Security Configuration Weaknesses:**
    - MFA authentication for the root account was false.
    - Multiple different access keys (ASIA4ZPZU3K4ZI76PDGS, ASIA4ZPZU3K4SXZNKRLP, etc.) were used, suggesting possible credential compromise.

Risk Assessment:

Threat Level: High
Potential Impact: Unauthorized access to AWS services, data exfiltration, privilege escalation.

Recommendations:

1. **Immediate Actions:**
    - **Revoke Active Sessions:** Immediately terminate all active AWS root sessions and revoke any active access keys.
    - **Restrict IP Access:** Block traffic from 178.153.40.80 at the firewall or AWS security groups.
    - **Enable MFA:** Immediately enable Multi-Factor Authentication (MFA) on the root account.
2. **Long-Term Security Measures:**
    - **Review IAM Policies:** Restrict the use of root credentials and create separate IAM roles with the least privilege.
    - **Monitor CloudTrail Logs:** Set up AWS CloudWatch alarms for failed login attempts and API calls from unrecognized IPs.
    - **Conduct Security Audit:** Perform an IAM access review to identify and remove unnecessary permissions.
    - **Rotate Access Keys:** Regularly rotate AWS IAM access keys and enforce key management best practices.

Conclusion:

The observed activities indicate potential unauthorized access attempts targeting AWS root credentials. The absence of MFA authentication on the root account significantly increases the risk. Immediate remediation steps, including session termination, MFA enforcement, and IAM security hardening, are necessary to mitigate risks and prevent future attacks.

Action Required: Implement recommended security measures and continuously monitor for suspicious activities.