Cybersecurity Incident Report

Date: March 22, 2025

Prepared by: Denis Mutwiri Gitonga

Affected Account: AWS Account ID: 075255217613

Incident Summary:

This report analyzes unusual activity recorded in AWS CloudTrail logs for the AWS root account (ID: 075255217613). The logs indicate multiple failed access attempts and suspicious API calls from an external IP address (176.202.8.177). Notably, Multi-Factor Authentication (MFA) was not enabled for the root user, increasing the risk of unauthorized access.

Findings: <u>1.0</u>

- **Event Source:** s3.amazonaws.com
- **Event Name:** GetBucketAcl
- **Response:** null
- **Timestamp:** 2025-03-22T07:00:14Z

1. **Infrastructure Insights:**
   - The domain uses AWS S3 for storing CloudTrail logs in the eu-north-1 region, indicating a logging setup for auditing AWS account activity.
   - The GetBucketAcl API call by CloudTrail suggests automated logging of bucket permissions, which is a standard practice for compliance and monitoring.

2. **Security Observations:**
   - Secure Communication: The use of TLS 1.3 and a secure cipher suite (TLS_AES_128_GCM_SHA256) ensures encrypted communication, reducing the risk of data interception.
   - CloudTrail Integration: The event being triggered by CloudTrail is a positive sign, as it indicates logging and monitoring are enabled for the AWS account.
   - No Direct User Involvement: Unlike the previous SNS alert, this event was initiated by CloudTrail, not a user, reducing the immediate risk of unauthorized access. However, the bucket's ACL permissions should be reviewed to ensure they are not overly permissive.

3. **Potential Risks:**
   - Bucket ACL Exposure: If the S3 bucket's ACL is misconfigured (e.g., public read access), it could expose sensitive CloudTrail logs, potentially revealing account activity or infrastructure details to attackers.
   - Reconnaissance Potential: The GetBucketAcl call could be part of a broader reconnaissance effort if initiated by an unauthorized party, though in this case, it appears to be a legitimate CloudTrail action.

```
"Records": [
  {
    "eventVersion": "1.11",
    "userIdentity": {
      "type": "AWSService",
      "invokedBy": "cloudtrail.amazonaws.com"
    },
    "eventTime": "2025-03-22T00:14:00Z",
    "eventSource": "s3.amazonaws.com",
    "eventName": "GetBucketAcl",
    "awsRegion": "eu-north-1",
    "sourceIPAddress": "cloudtrail.amazonaws.com",
    "userAgent": "cloudtrail.amazonaws.com",
    "requestParameters": {
      "bucketName": "aws-cloudtrail-logs-075255217613-8482ae85",
      "Host": "aws-cloudtrail-logs-075255217613-8482ae85.s3.eu-north-1.amazonaws.com",
      "acl": ""
    },
    "responseElements": null,
    "additionalEventData": {
      "SignatureVersion": "SigV4",
      "CipherSuite": "TLS_AES_128_GCM_SHA256",
      "bytesTransferredIn": 0,
      "AuthenticationMethod": "AuthHeader",
      "x-amz-id-2": "TsESDsds7jJM2MzFv8OI5ILj1qHZ2ptMlw+R/0IOP570kPpvHLmkglb0LMHoDrwTCVmPX43oyv0RjRR4PKQJfiU/zN
      "bytesTransferredOut": 480
    },
    "requestID": "JRBPAVNB2Y37JQK4",
    "eventID": "2466c862-90f2-3e89-91f8-d5bddcb095f1",
    "readOnly": true,
    "resources": [
      {
        "accountId": "075255217613",
        "type": "AWS::S3::Bucket",
        "ARN": "arn:aws:s3:::aws-cloudtrail-logs-075255217613-8482ae85"
      }
    ],
    "eventType": "AwsApiCall",
    "managementEvent": true,
    "recipientAccountId": "075255217613",
    "sharedEventID": "67fd5cb2-5d78-4147-af45-5062ea9e7376",
    "eventCategory": "Management"
  }
```


2.0

- **Event Source:** ec2.amazonaws.com
- **Event Name:** DescribeRegions

- **Response:** null
- **Timestamp:** 2025-03-22T00:16:40Z

I. Infrastructure Insights:

- This alert is a duplicate of the first SNS alert analyzed, confirming the same DescribeRegions API call on the same EC2 instance in eu-north-1. The consistency across alerts reinforces that halisans.com relies on AWS EC2 for hosting.
- The source IP (176.202.8.177) and user agent (Chrome on Windows 10) are identical, suggesting the same client or user is interacting with the AWS environment**.**

II. Security Concerns:

- Root Account Usage: The repeated use of the root account for API calls remains a critical risk. Root accounts have unrestricted access, making them a prime target for attackers.
- Lack of MFA: The absence of MFA on the root account, as noted in the first alert, continues to heighten the risk of credential compromise.
- Potential Reconnaissance: The DescribeRegions call, while potentially legitimate, could indicate reconnaissance if performed by an unauthorized party. The repetition of this call may suggest ongoing activity.

III. Positive Aspects:

- The use of TLS 1.3 and a secure cipher suite (TLS_AES_128_GCM_SHA256) ensures encrypted communication, consistent with prior findings.
- The session originates from a modern browser, indicating up-to-date client software.

```
  "recipientAccountId": "075255217613",
  "eventCategory": "Management",
  "tlsDetails": {
    "tlsVersion": "TLSv1.3",
    "cipherSuite": "TLS_AES_128_GCM_SHA256",
    "clientProvidedHostHeader": "ec2.eu-north-1.amazonaws.com"
  },
  "sessionCredentialFromConsole": "true"
}
```

```
{
    "eventVersion": "1.10",
    "userIdentity": {
      "type": "Root",
      "principalId": "075255217613",
      "arn": "arn:aws:iam::075255217613:root",
      "accountId": "075255217613",
      "accessKeyId": "ASIARDBMPPXG2AYJQOYF",
      "sessionContext": {
        "attributes": {
          "creationDate": "2025-03-21T21:58:32Z",
          "mfaAuthenticated": "false"
        }
      }
    },
    "eventTime": "2025-03-22T00:16:40Z",
    "eventSource": "ec2.amazonaws.com",
    "eventName": "DescribeRegions",
    "awsRegion": "eu-north-1",
    "sourceIPAddress": "176.202.8.177",
    "userAgent": "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/134.0.0.0 S
    "requestParameters": {
      "regionSet": {},
      "allRegions": true
    },
    "responseElements": null,
    "requestID": "a1a4ff40-97a7-452a-8600-08e3c8cd3594",
    "eventID": "67399557-7793-422e-bd14-4ca5bc9f3d75",
    "readOnly": true,
    "eventType": "AwsApiCall",
    "managementEvent": true,
    "recipientAccountId": "075255217613",
```


Risk Assessment:

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

Recommendations:

I. **Review S3 Bucket Permissions:**

- Ensure the S3 bucket (aws-cloudtrail-logs-075255217613-8482ae85) has strict access controls. Use AWS S3 Block Public Access and verify the ACL does not allow public or unauthorized access.

- Implement least-privilege IAM policies for accessing the bucket, restricting permissions to only necessary services and users.

II. **Enhance CloudTrail Security**:

- Enable encryption for CloudTrail logs using AWS Key Management Service (KMS) to protect log data at rest.
- Set up CloudTrail log file validation to detect tampering and ensure log integrity.

III. Secure the Root Account:

- Disable Root Access: Avoid using the root account for daily operations. Create IAM users with least-privilege permissions for administrative tasks.
- Enable MFA: Immediately enable multi-factor authentication (MFA) on the root account to prevent unauthorized access if credentials are compromised.

IV. Monitor and Audit API Calls:

- Enable AWS CloudTrail to log all API calls, including DescribeRegions, for better visibility into account activity.
- Set up CloudWatch alarms to alert on suspicious API activity, such as repeated root account usage or unusual region queries.

Conclusion:

The AWS SNS alert indicates;

- ✓ A secure, CloudTrail-initiated GetBucketAcl API call on an S3 bucket in the eu-north-1 region, used for storing CloudTrail logs.
- ✓ The use of TLS 1.3 and secure authentication is a positive sign, but the bucket's ACL permissions should be reviewed to prevent potential exposure of sensitive logs.
- ✓ DescribeRegions API call on an EC2 instance in the eu-north-1 region, initiated by the root account without MFA
- ✓ Implementing the recommended measures—securing S3 permissions, enhancing CloudTrail security, and monitoring API activity—will further strengthen the domain's AWS environment.
- ✓ The repeated use of the root account and lack of MFA continue to pose significant risks, potentially exposing the account to unauthorized access or reconnaissance. Implementing the recommended measures—disabling root access, enabling MFA, and monitoring API activity—remains critical to securing the AWS environment.

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