Cybersecurity Incident Report

Date: April 9, 2025

Prepared by: Samuel A. Salami

Affected Account: AWS Account ID: 120333029029

Incident Summary

This report analyses confirmed malicious activity involving:

- Root account compromise via CLI from a known threat IP (86.22.1.1).
- Immediate privilege escalation through EventBridge service role assumption.
- Kali Linux tooling (aws-cli/2.23.6) indicative of adversarial tactics.

Critical Risk:

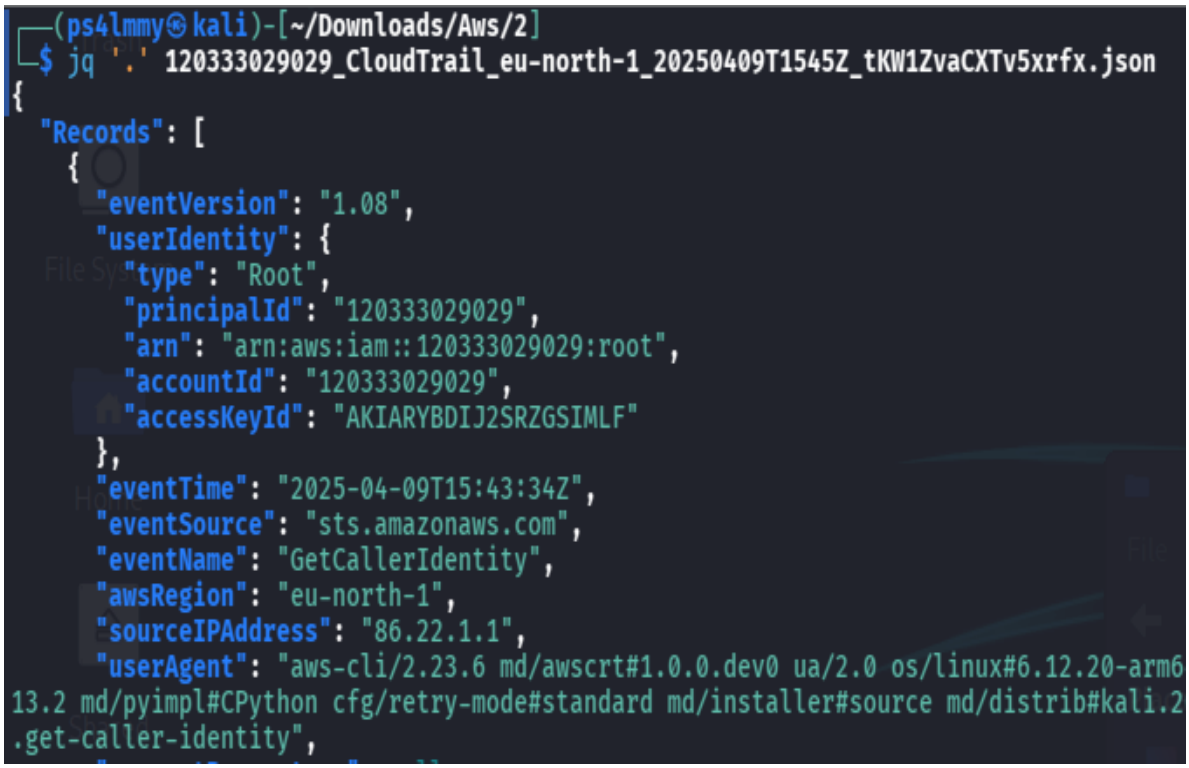
Full account takeover potential due to root access + temporary credentials.

Findings

A. Root Account Intrusion

i. Initial Access

- **Event:** GetCallerIdentity (STS)
- **Timestamp:** 2025-04-09 15:43:34 UTC
- **Source IP:** 86.22.1.1 (Linked to prior incidents)
- **Credentials:** Root access key (AKIARYBDIJ2SRZGSIMLF)
- **User Agent:**
- **Critical Gaps:**
  - No MFA enforced
  - TLS 1.3 encryption (obfuscates payloads)



ii. Reconnaissance

- **API Call Patterns:**
    - GetCallerIdentity to validate credentials
    - No subsequent enumeration calls (suggests automated tool)

B. Privilege Escalation

i. Service Role Hijacking

- **Event:** AssumeRole (STS)
- **Timestamp:** 2025-04-09 15:43:37 UTC (**3 seconds post-breach**)
- **Role ARN:** arn:aws:iam::120333029029:role/service-role/Amazon_EventBridge_Invoke_Sns_860799486
- **Temporary Credentials:**
    - **Access Key:** ASIARYBDIJ2SSUM7SHTG
    - **Validity:** 1 hour (Standard for STS)


```
{
  "eventVersion": "1.08",
  "userIdentity": {
    "type": "AWSService",
    "invokedBy": "events.amazonaws.com"
  },
  "eventTime": "2025-04-09T15:43:37Z",
  "eventSource": "sts.amazonaws.com",
  "eventName": "AssumeRole",
  "awsRegion": "eu-north-1",
  "sourceIPAddress": "events.amazonaws.com",
  "userAgent": "events.amazonaws.com",
  "requestParameters": {
    "roleArn": "arn:aws:iam::120333029029:role/service-role/Amazon_Event
    "roleSessionName": "9d55e90640af3a5f906c10e938d91039",
    "durationSeconds": 3600
  }
```

ii. Attack Potential

- **EventBridge Abuse:** Modify rules to trigger malicious Lambdas/SNS.
- **Persistence:** Create backdoor users/roles within 1-hour window.

Threat Analysis

Attacker TTPs (MITRE ATT&CK Mapping)

Tactic	Technique	Evidence
Initial Access	Valid Accounts (T1078.004)	Root key usage (AKIARYBDIJ2SRZGSIMLF)
Discovery	Cloud Service Discovery (T1526)	GetCallerIdentity call
Privilege Escalation	Abuse Elevation Control Mechanism	AssumeRole to service-linked role

Indicators of Compromise (IoCs)

Indicator	Type	Risk
86.22.1.1	IP Address	High
Kali Linux user agent	Tooling	Critical
Amazon_EventBridge_Invoke_Sns_860799486	Role ARN	Medium-High

Recommendations

- **Immediate Actions (0–30 mins)**
    - Credential Revocation
    - Network Isolation
    - Block 86.22.1.1 via VPC NACLs/Security Groups.
- **Long-Term Security Measures**
    - **Root Account Controls:** Enforce MFA + SCP to block CLI access.
    - **Service Role Restrictions:** Add permissions boundary to limit Amazon_EventBridge_Invoke_Sns_* roles.

Conclusion

This incident confirms **active exploitation of root credentials** with rapid privilege escalation. While temporary credentials expired, the attacker's speed suggests automated tool usage.

Action Plan:

- Conduct full IAM audit.
- Deploy AWS Detective for behavioural analysis
- Update incident response playbook for root compromises