
GENERAL:

First Seen Time and Date: 22/08/2025 01:56:47 +0500
Insight: Insight-17933 - Collection with Privilege Escalation and Execution

Associated Signals:

1. AWS CloudTrail - Logging Configuration Change Observed
2. Spike in AWS API Call from User
3. Spike in AWS API Call from User
4. AWS CloudTrail - Public S3 Bucket Exposed
5. Spike in AWS API Call from User
6. AWS S3 Operation performed by jschmo-sa

SEVERITY CLASSIFICATION:

Priority: P1

Reason: This incident is classified as **P1 Critical** because the attacker (user jschmo-sa) has successfully escalated privileges and engaged in high-risk behaviors, including **modifying AWS CloudTrail logs (defense evasion), exposing S3 buckets publicly (potential data exposure), and executing suspicious API activity at scale**. These actions strongly indicate active compromise, attempted persistence, and possible staging for **data exfiltration**. The combination of privilege escalation, logging tampering, and cloud resource modification requires **immediate response**.

SOURCE DETAILS:

Source IP: 50.200.63.82
Device IP: 107.207.37.56
Source Username: jschmo-sa
Application: cloudtrail.amazonaws.com
Event: UpdateTrail (CloudTrail logging configuration change)

MITRE ATT&CK Techniques Observed:

- **T1562.008 - Impair Defenses: Disable or Modify Cloud Logs**
- **T1578 - Modify Cloud Compute Infrastructure**

- **T1489 - Service Stop**
- **T1562 - Impair Defenses**
- **T1578.004 - Revert Cloud Instance**
- **Tactics:** TA0002 - Execution, TA0005 - Defense Evasion

TARGET DETAILS:

Target Username: jschmo-sa
Target Email Address: *N/A (service account)*
Target IP: 107.207.37.56
Target Location: US-based IP (likely AWS infrastructure)

ADDITIONAL INFORMATION:

- API call observed: **UpdateTrail** (attempted to modify or disable logging on CloudTrail).
- **Public S3 bucket exposure** increases the risk of sensitive data leakage.
- **Multiple spikes in AWS API calls** indicate potential automated reconnaissance or exploitation activity.

INCIDENT DETAILS:

Between **22/08/2025 01:56 and onwards**, the service account jschmo-sa initiated suspicious AWS operations suggestive of compromise.

1. The first observed malicious activity was an **UpdateTrail API call** via cloudtrail.amazonaws.com, attempting to **modify or disable CloudTrail logging** — a common defense evasion tactic (T1562.008).
2. Following this, multiple **spikes in AWS API calls** were executed from the same user account, consistent with **scripted or automated activity**.
3. A **public S3 bucket exposure** event was logged, significantly raising the risk of data collection and exfiltration.
4. The service account continued activity associated with **execution and collection**, as evidenced by suspicious S3 operations and CloudTrail modifications.

This sequence of events confirms the account jschmo-sa was abused to gain elevated privileges, impair visibility, and stage cloud resources for exploitation.

REMEDIATION ACTIONS:

Immediate Steps:

- Revoke all credentials (API keys, session tokens) for jschmo-sa and enforce MFA on the account.
- Suspend or disable the affected IAM account until investigation is complete.
- Block suspicious source IP **50.200.63.82** at the firewall/VPC level.
- Investigate **107.207.37.56** (CloudTrail device endpoint) for abnormal activity.

Forensic & Containment:

- Review all CloudTrail logs to identify additional **logging tampering attempts**.
- Audit **S3 buckets** for unauthorized policy changes, exposed data, or persistence mechanisms.
- Check for newly created IAM roles, access keys, or backdoors.
- Investigate other accounts for similar anomalous API activity.

Long-Term Security Measures:

- Enforce **least privilege** access across IAM accounts.
- Enable **CloudTrail log file integrity validation** and send logs to a secure, immutable storage location (e.g., dedicated security S3 bucket with restricted access).
- Configure **AWS GuardDuty, Security Hub, and Detective** for continuous detection of IAM anomalies.
- Conduct a **user awareness session** for administrators on safe credential management.
- Rotate credentials for any AWS resources accessible by jschmo-sa.
