TITAN AI · CONDUIT · INCIDENT

INC0010008 — [TITAN] High — security on iam-user-svc-backup

Severity	High	Priority	3 - Moderate
Cloud	AWS	State	New
Resource	iam-user-svc-backup	Group	identity_and_access
Resource type	AWS::IAM::User	Change type	Incident
Opened	2026-04-21 15:28:19	Closed	2026-04-21 15:28:19
CAB required	Yes	Close code	—

Security Finding

```
IAM user 'iam-user-svc-backup' has MFA disabled and 180-day-old access keys. Human service account posture non-compliant with CIS_AWS_1.14.
```

Justification

```
High: IAM user 'iam-user-svc-backup' has MFA disabled and 180-day-old access keys. Human service account posture non-compliant with CIS_AWS_1.14.
```

Implementation Plan

```
1. Pre-change snapshot captured by TITAN (auto-rollback available).
2. Execute fix command:
aws iam update-access-key --user-name iam-user-svc-backup --access-key-id AKIA... --status Inactive; aws iam create-access-key --user-name iam-user-svc-backup; rotate credentials in callers within 24h.
3. TITAN FORGE verifies the fix was applied.
4. Post-change rescan by TITAN SCOUT — finding must no longer appear.
5. Close ticket with Successful close_code.
```

Risk & Impact Analysis

```
Risk level: MEDIUM-HIGH risk — misconfiguration with realistic exploit path.
Business impact if unremediated: Increases attack surface; auditor finding likely.
Scope: single resource (iam-user-svc-backup).
Blast radius: change is idempotent; pre-change snapshot captured by TITAN; auto-rollback available if rescan fails.
Finding detail: IAM user 'iam-user-svc-backup' has MFA disabled and 180-day-old access keys. Human service account posture non-compliant with CIS_AWS_1.14.
```

Backout / Rollback Plan

```
1. TITAN auto-captured snapshot of iam-user-svc-backup before change (baseline: titan-killer-20260421T222819Z).
2. If post-change rescan still shows the finding OR a new issue appears within 15 min:
a. TITAN FORGE fires rollback automatically using stored snapshot.
b. Incident reopens and escalates to on-call.
3. Manual rollback command path (human override) is documented in close notes.
```

Test Plan

```
1. TITAN SCOUT rescans iam-user-svc-backup immediately after FORGE applies the change.
2. PASS criteria: the specific finding no longer appears in SCOUT results.
```

3. PASS criteria: no new CRITICAL or HIGH findings introduced by the change.
4. Automated compliance check: HIPAA/PCI/SOC2 controls re-evaluated.
5. If any check fails, backout plan fires automatically.

Recommended Fix Command

```
aws iam update-access-key --user-name iam-user-svc-backup --access-key-id AKIA... --status Inactive; aws iam create-access-key --user-name iam-user-svc-backup; rotate credentials in callers within 24h.
```

Compliance Mapping

CIS 1.x IAM, NIST AC-2, SOC 2 CC6.1, PCI DSS 3.5

AI Close Notes

2026-04-21 15:28:19 - System Administrator (Work notes)
[TITAN CONDUIT] Incident auto-filed from security scan.
Detecting agent: unknown (scan titan-killer-20260421T222819Z).
Severity: High (priority 2).
This is a hygiene/access-control issue that does not require a CAB-gated change window. Assign to the listed team and resolve per their standard runbook. TITAN will auto-detect clearance on the next scan.