CHG0030113 — [TITAN] Medium — storage on s3-telco-radius-logs

Severity	Medium	Priority	3 - Moderate
Cloud	AWS	State	Assigned
Resource	s3-telco-radius-logs	Group	infrastructure_operations
Resource type	AWS::S3::Bucket	Change type	Normal
Opened	2026-04-22 19:01:25	Closed	2026-04-22 19:01:25
CAB required	No	Close code	—

Security Finding

```
RADIUS session log bucket lacks MFA-delete. An attacker with IAM key could purge authentication
evidence.
```

Justification

```
Medium: RADIUS session log bucket lacks MFA-delete. An attacker with IAM key could purge
authentication evidence.
```

Implementation Plan

```
1. Pre-change snapshot captured by TITAN (auto-rollback available).
2. Execute fix command:
aws s3api put-bucket-versioning --bucket s3-telco-radius-logs --versioning-configuration
Status=Enabled,MFADelete=Enabled --mfa 'arn:aws:iam::ACCT:mfa/rootUser 123456'
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 risk — weaker control, should be hardened.
Business impact if unremediated: Control weakness that compounds with other gaps.
Scope: single resource (s3-telco-radius-logs).
Blast radius: change is idempotent; pre-change snapshot captured by TITAN; auto-rollback available
if rescan fails.
Finding detail: RADIUS session log bucket lacks MFA-delete. An attacker with IAM key could purge
authentication evidence.
```

Backout / Rollback Plan

```
1. TITAN auto-captured snapshot of s3-telco-radius-logs before change (baseline:
titan-telecom-demo-20260422T201925Z).
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 s3-telco-radius-logs 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 s3api put-bucket-versioning --bucket s3-telco-radius-logs --versioning-configuration
Status=Enabled,MFADelete=Enabled --mfa 'arn:aws:iam::ACCT:mfa/rootUser 123456'
```

Compliance Mapping

```
HIPAA §164.312(e)(1), PCI DSS 3.4, SOC 2 CC6.1, CIS 1.x IAM
```

AI Close Notes

```
TITAN CONDUIT opened this medium storage change request and assigned it to the regulatory_affairs
group for review. STATE: ASSIGNED — awaiting human action. Per TITAN AI policy (and Kazmi rule,
2026-04-22), configuration changes are NEVER auto-applied and change tickets are NEVER auto-closed
by TITAN. The assigned group reviews the recommended fix, schedules a CAB-approved change window,
applies the fix manually, validates via SCOUT rescan, and closes this ticket themselves. TITAN
documents and routes — the human owns the change from here.
```