TITAN AI · CONDUIT · INCIDENT

INC0010108 — [TITAN] High — data_leak on s3-telco-billing-exports

Severity	High	Priority	2 - High
Cloud	AWS	State	Closed
Resource	s3-telco-billing-exports	Group	security_engineering
Resource type	AWS::S3::Bucket	Change type	Incident
Opened	2026-04-22 19:31:25	Closed	2026-04-22 19:45:25
CAB required	Yes	Close code	Successful

Security Finding

```
Billing-export S3 bucket public-read ACL detected by CONDUIT scan — monthly bills with customer PII/location data were reachable unauthenticated. FCC CPNI §222 breach condition.
```

Justification

```
High: Billing-export S3 bucket public-read ACL detected by CONDUIT scan — monthly bills with customer PII/location data were reachable unauthenticated. FCC CPNI §222 breach condition.
```

Implementation Plan

```
1. Pre-change snapshot captured by TITAN (auto-rollback available).
2. Execute fix command:
aws s3api put-public-access-block --bucket s3-telco-billing-exports
--public-access-block-configuration
BlockPublicAcls=true,IgnorePublicAcls=true,BlockPublicPolicy=true,RestrictPublicBuckets=true &&
aws s3api put-bucket-acl --bucket s3-telco-billing-exports --acl private
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 (s3-telco-billing-exports).
Blast radius: change is idempotent; pre-change snapshot captured by TITAN; auto-rollback available
if rescan fails.
Finding detail: Billing-export S3 bucket public-read ACL detected by CONDUIT scan — monthly bills
with customer PII/location data were reachable unauthenticated. FCC CPNI §222 breach condition.
```

Backout / Rollback Plan

```
1. TITAN auto-captured snapshot of s3-telco-billing-exports 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-billing-exports 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-public-access-block --bucket s3-telco-billing-exports
--public-access-block-configuration
BlockPublicAcls=true,IgnorePublicAcls=true,BlockPublicPolicy=true,RestrictPublicBuckets=true &&
aws s3api put-bucket-acl --bucket s3-telco-billing-exports --acl private
```

Compliance Mapping

```
HIPAA §164.312(e)(1), PCI DSS 3.4, SOC 2 CC6.1, CIS Azure 6.2
```

AI Close Notes

```
TITAN CONDUIT orchestrated end-to-end: SCOUT detected the high data_leak incident, FORGE applied
the consent-gated fix automatically (incident class), SCOUT rescan confirmed the finding cleared,
and CONDUIT closed this ticket with a Successful close_code. Pre-change snapshot retained for 30
days for rollback.
```