

CHG0030006 — [TITAN] Critical — security on s3-titan-customer-exports

Severity	Critical	Priority	1 - Critical
Cloud	AWS	State	New
Resource	s3-titan-customer-exports	Group	infrastructure_operations
Resource type	AWS::S3::Bucket	Change type	Normal
Opened	2026-04-21 14:36:43	Closed	2026-04-21 14:36:43
CAB required	Yes	Close code	—

Security Finding

S3 bucket 's3-titan-customer-exports' has publicly accessible objects via BlockPublicAcls=false – exports of customer PII are exposed.

Justification

S3 bucket 's3-titan-customer-exports' has publicly accessible objects via BlockPublicAcls=false – exports of customer PII are exposed.

Implementation Plan

1. Pre-change snapshot captured by TITAN (auto-rollback available).
2. Execute fix command:
`aws s3api put-public-access-block --bucket s3-titan-customer-exports --public-access-block-configuration BlockPublicAcls=true,BlockPublicPolicy=true,IgnorePublicAcls=true,RestrictPublicBuckets=true`
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: HIGH business risk – active exposure; fix required immediately.
Business impact if unremediated: Potential data exfil, privilege escalation, or compliance breach.
Scope: single resource (s3-titan-customer-exports).
Blast radius: change is idempotent; pre-change snapshot captured by TITAN; auto-rollback available if rescan fails.
Finding detail: S3 bucket 's3-titan-customer-exports' has publicly accessible objects via BlockPublicAcls=false – exports of customer PII are exposed.

Backout / Rollback Plan

1. TITAN auto-captured snapshot of s3-titan-customer-exports before change (baseline: titan-live-demo-20260421T213642Z).
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-titan-customer-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-titan-customer-exports
--public-access-block-configuration
BlockPublicAcls=true,BlockPublicPolicy=true,IgnorePublicAcls=true,RestrictPublicBuckets=true
```

Compliance Mapping

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

AI Close Notes

(empty)