CHG0030008 — [TITAN] High — security on gs-titan-logs

Severity	High	Priority	2 - High
Cloud	GCP	State	New
Resource	gs-titan-logs	Group	infrastructure_operations
Resource type	storage.googleapis.com/Bucket	Change type	Normal
Opened	2026-04-21 14:36:44	Closed	2026-04-21 14:36:44
CAB required	Yes	Close code	—

Security Finding

```
GCS bucket 'gs-titan-logs' has allUsers with Storage Object Viewer — logs containing request IDs
and internal endpoints are publicly readable.
```

Justification

```
GCS bucket 'gs-titan-logs' has allUsers with Storage Object Viewer — logs containing request IDs
and internal endpoints are publicly readable.
```

Implementation Plan

```
1. Pre-change snapshot captured by TITAN (auto-rollback available).
2. Execute fix command:
gcloud storage buckets remove-iam-policy-binding gs://gs-titan-logs --member=allUsers
--role=roles/storage.objectViewer
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 (gs-titan-logs).
Blast radius: change is idempotent; pre-change snapshot captured by TITAN; auto-rollback available
if rescan fails.
Finding detail: GCS bucket 'gs-titan-logs' has allUsers with Storage Object Viewer — logs
containing request IDs and internal endpoints are publicly readable.
```

Backout / Rollback Plan

```
1. TITAN auto-captured snapshot of gs-titan-logs 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 gs-titan-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

```
gcloud storage buckets remove-iam-policy-binding gs://gs-titan-logs --member=allUsers
--role=roles/storage.objectViewer
```

Compliance Mapping

```
HIPAA §164.312(e)(1), PCI DSS 3.4, SOC 2 CC6.1, SOC 2 CC7.1
```

AI Close Notes

```
(empty)
```