CHG0030009 — [TITAN] Critical — security on csql-titan-orders

Severity	Critical	Priority	1 - Critical
Cloud	Multi	State	New
Resource	csql-titan-orders	Group	database_operations
Resource type	compute.googleapis.com/DBInstance	Change type	Normal
Opened	2026-04-21 14:36:44	Closed	2026-04-21 14:36:44
CAB required	Yes	Close code	—

Security Finding

```
Cloud SQL 'csql-titan-orders' has ssl_mode=ALLOW (accepts unencrypted connections) and no
customer-managed encryption key — order data at rest is only provider-encrypted.
```

Justification

```
Cloud SQL 'csql-titan-orders' has ssl_mode=ALLOW (accepts unencrypted connections) and no
customer-managed encryption key — order data at rest is only provider-encrypted.
```

Implementation Plan

```
1. Pre-change snapshot captured by TITAN (auto-rollback available).
2. Execute fix command:
gcloud sql instances patch csql-titan-orders --require-ssl --disk-encryption-key-name=projects/ti
tan-ai-prod-882017/locations/us-central1/keyRings/titan-kr/cryptoKeys/titan-db-key
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 (csql-titan-orders).
Blast radius: change is idempotent; pre-change snapshot captured by TITAN; auto-rollback available
if rescan fails.
Finding detail: Cloud SQL 'csql-titan-orders' has ssl_mode=ALLOW (accepts unencrypted connections)
and no customer-managed encryption key — order data at rest is only provider-encrypted.
```

Backout / Rollback Plan

```
1. TITAN auto-captured snapshot of csql-titan-orders 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 csql-titan-orders 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 sql instances patch csql-titan-orders --require-ssl --disk-encryption-key-name=projects/titan-ai-prod-882017/locations/us-central1/keyRings/titan-kr/cryptoKeys/titan-db-key
```

Compliance Mapping

```
HIPAA §164.312(e)(1), PCI DSS 3.4, SOC 2 CC6.1, PCI DSS 3.5
```

AI Close Notes

```
(empty)
```