# CHG0030104 — [TITAN] High — database on rds-pci-card-data

| | | | |
|---|---|---|---|
| Severity | High | Priority | 2 - High |
| Cloud | AWS | State | Assigned |
| Resource | rds-pci-card-data | Group | database_operations |
| Resource type | AWS::RDS::DBInstance | Change type | Normal |
| Opened | 2026-04-22 19:55:22 | Closed | 2026-04-22 19:55:22 |
| CAB required | Yes | Close code | — |

## Security Finding

```
PCI card-data RDS instance has 'publicly_accessible=true' set — violates PCI DSS 1.3.4 (no direct public access to CHD). TLS also disabled (rds.force_ssl=0).
```

## Justification

```
High: PCI card-data RDS instance has 'publicly_accessible=true' set — violates PCI DSS 1.3.4 (no direct public access to CHD). TLS also disabled (rds.force_ssl=0).
```

## Implementation Plan

```
1. Pre-change snapshot captured by TITAN (auto-rollback available).
2. Execute fix command:
aws rds modify-db-instance --db-instance-identifier rds-pci-card-data --no-publicly-accessible
--apply-immediately && aws rds modify-db-parameter-group --db-parameter-group-name pci-card-pg
--parameters "ParameterName=rds.force_ssl,ParameterValue=1,ApplyMethod=immediate"
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 (rds-pci-card-data).
Blast radius: change is idempotent; pre-change snapshot captured by TITAN; auto-rollback available
if rescan fails.
Finding detail: PCI card-data RDS instance has 'publicly_accessible=true' set — violates PCI DSS
1.3.4 (no direct public access to CHD). TLS also disabled (rds.force_ssl=0).
```

## Backout / Rollback Plan

```
1. TITAN auto-captured snapshot of rds-pci-card-data before change (baseline:
titan-banking-demo-20260422T201922Z).
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 rds-pci-card-data 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 rds modify-db-instance --db-instance-identifier rds-pci-card-data --no-publicly-accessible
--apply-immediately && aws rds modify-db-parameter-group --db-parameter-group-name pci-card-pg
--parameters "ParameterName=rds.force_ssl,ParameterValue=1,ApplyMethod=immediate"
```

## 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 high database change request and assigned it to the banking_compliance
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.
```