CHG0030007 — [TITAN] High — security on sg-titan-rds

Severity	High	Priority	2 - High
Cloud	AWS	State	New
Resource	sg-titan-rds	Group	security_engineering
Resource type	AWS::EC2::SecurityGroup	Change type	Normal
Opened	2026-04-21 14:36:43	Closed	2026-04-21 14:36:43
CAB required	Yes	Close code	—

Security Finding

```
Security group 'sg-titan-rds' allows MySQL (port 3306) from 0.0.0.0/0 — RDS is directly exposed to the internet. Firewall policy violation.
```

Justification

```
Security group 'sg-titan-rds' allows MySQL (port 3306) from 0.0.0.0/0 — RDS is directly exposed to the internet. Firewall policy violation.
```

Implementation Plan

```
1. Pre-change snapshot captured by TITAN (auto-rollback available).
2. Execute fix command:
aws ec2 revoke-security-group-ingress --group-id sg-0a1b2c3d --protocol tcp --port 3306 --cidr 0.0.0.0/0
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 (sg-titan-rds).
Blast radius: change is idempotent; pre-change snapshot captured by TITAN; auto-rollback available if rescan fails.
Finding detail: Security group 'sg-titan-rds' allows MySQL (port 3306) from 0.0.0.0/0 — RDS is directly exposed to the internet. Firewall policy violation.
```

Backout / Rollback Plan

```
1. TITAN auto-captured snapshot of sg-titan-rds 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 sg-titan-rds 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 ec2 revoke-security-group-ingress --group-id sg-0a1b2c3d --protocol tcp --port 3306 --cidr 0.0.0.0/0
```

Compliance Mapping

```
CIS Azure 6.2, NIST SC-7, PCI DSS 1.2.1
```

AI Close Notes

```
(empty)
```