

CHG0030105 — [TITAN] High — network on sg-banking-webtier-prod

Severity	High	Priority	2 - High
Cloud	AWS	State	Assigned
Resource	sg-banking-webtier-prod	Group	network_operations
Resource type	AWS::EC2::SecurityGroup	Change type	Normal
Opened	2026-04-22 19:49:22	Closed	2026-04-22 19:49:22
CAB required	Yes	Close code	—

Security Finding

Security group sg-banking-webtier-prod allows 0.0.0.0/0 on port 3306 (MySQL) – production banking DB exposed to internet. PCI DSS 1.2.1 firewall/router configuration violation.

Justification

High: Security group sg-banking-webtier-prod allows 0.0.0.0/0 on port 3306 (MySQL) – production banking DB exposed to internet. PCI DSS 1.2.1 firewall/router configuration 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-0abc123 --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-banking-webtier-prod).
Blast radius: change is idempotent; pre-change snapshot captured by TITAN; auto-rollback available if rescan fails.
Finding detail: Security group sg-banking-webtier-prod allows 0.0.0.0/0 on port 3306 (MySQL) – production banking DB exposed to internet. PCI DSS 1.2.1 firewall/router configuration violation.

Backout / Rollback Plan

1. TITAN auto-captured snapshot of sg-banking-webtier-prod 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 sg-banking-webtier-prod 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-0abc123 --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

TITAN CONDUIT opened this high network 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.

TITAN AI LLC · CONDUIT Agent · Patent Pending USPTO 19/645,524 · Generated 2026-04-22 20:19 UTC