CHG0030102 — [TITAN] High — firewall on sg-telco-roaming-api

Severity	High	Priority	2 - High
Cloud	AWS	State	Assigned
Resource	sg-telco-roaming-api	Group	network_operations
Resource type	AWS::EC2::SecurityGroup	Change type	Normal
Opened	2026-04-22 20:07:25	Closed	2026-04-22 20:07:25
CAB required	Yes	Close code	—

Security Finding

```
Roaming partner API security group allows 0.0.0.0/0 on port 443 AND port 80. Should be restricted to GRX/IPX partner IP ranges only per GSMA PRD IR.77.
```

Justification

```
High: Roaming partner API security group allows 0.0.0.0/0 on port 443 AND port 80. Should be restricted to GRX/IPX partner IP ranges only per GSMA PRD IR.77.
```

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-telco-roaming --protocol tcp --port 80 --cidr 0.0.0.0/0 && aws ec2 authorize-security-group-ingress --group-id sg-telco-roaming --protocol tcp --port 443 --cidr 195.35.192.0/22
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-telco-roaming-api).
Blast radius: change is idempotent; pre-change snapshot captured by TITAN; auto-rollback available if rescan fails.
Finding detail: Roaming partner API security group allows 0.0.0.0/0 on port 443 AND port 80. Should be restricted to GRX/IPX partner IP ranges only per GSMA PRD IR.77.
```

Backout / Rollback Plan

```
1. TITAN auto-captured snapshot of sg-telco-roaming-api before change (baseline: titan-telecom-demo-20260422T201925Z).
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-telco-roaming-api 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-telco-roaming --protocol tcp --port 80 --cidr 0.0.0.0/0 && aws ec2 authorize-security-group-ingress --group-id sg-telco-roaming --protocol tcp --port 443 --cidr 195.35.192.0/22
```

Compliance Mapping

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

AI Close Notes

```
TITAN CONDUIT opened this high firewall change request and assigned it to the regulatory_affairs 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.
```