CHG0030101 — [TITAN] Critical — dns on r53-customer-portal

Severity	Critical	Priority	1 - Critical
Cloud	AWS	State	Assigned
Resource	r53-customer-portal	Group	network_operations
Resource type	AWS::Route53::HostedZone	Change type	Emergency
Opened	2026-04-22 20:13:25	Closed	2026-04-22 20:13:25
CAB required	Yes	Close code	—

Security Finding

```
Route 53 hosted zone r53-customer-portal lacks DNSSEC — telco customer portal DNS susceptible to cache-poisoning. FCC CPNI rules require reasonable security for customer-facing systems.
```

Justification

```
Critical: Route 53 hosted zone r53-customer-portal lacks DNSSEC — telco customer portal DNS susceptible to cache-poisoning. FCC CPNI rules require reasonable security for customer-facing systems.
```

Implementation Plan

```
1. Pre-change snapshot captured by TITAN (auto-rollback available).
2. Execute fix command:
aws route53 enable-hosted-zone-dnssec --hosted-zone-id Z012345ABC && aws route53 create-key-signing-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 (r53-customer-portal).
Blast radius: change is idempotent; pre-change snapshot captured by TITAN; auto-rollback available if rescan fails.
Finding detail: Route 53 hosted zone r53-customer-portal lacks DNSSEC — telco customer portal DNS susceptible to cache-poisoning. FCC CPNI rules require reasonable security for customer-facing systems.
```

Backout / Rollback Plan

```
1. TITAN auto-captured snapshot of r53-customer-portal 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 r53-customer-portal 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 route53 enable-hosted-zone-dnssec --hosted-zone-id Z012345ABC && aws route53
create-key-signing-key ...
```

Compliance Mapping

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

AI Close Notes

```
TITAN CONDUIT opened this critical dns 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.
```