

CHG0030105 — [TITAN] High — logging on app-telco-provisioning

Severity	High	Priority	2 - High
Cloud	Azure	State	Assigned
Resource	app-telco-provisioning	Group	observability_engineering
Resource type	Microsoft.Web/sites	Change type	Normal
Opened	2026-04-22 19:49:25	Closed	2026-04-22 19:49:25
CAB required	Yes	Close code	—

Security Finding

Subscriber provisioning app has application logs set to 'Off' – number-porting audit trail is missing. FCC number-portability rules require traceable provisioning events.

Justification

High: Subscriber provisioning app has application logs set to 'Off' – number-porting audit trail is missing. FCC number-portability rules require traceable provisioning events.

Implementation Plan

1. Pre-change snapshot captured by TITAN (auto-rollback available).
2. Execute fix command:
`az webapp log config --resource-group rg-telco-prov --name app-telco-provisioning --application-logging true --level information --retention-in-days 2555`
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 (app-telco-provisioning).
Blast radius: change is idempotent; pre-change snapshot captured by TITAN; auto-rollback available if rescan fails.
Finding detail: Subscriber provisioning app has application logs set to 'Off' – number-porting audit trail is missing. FCC number-portability rules require traceable provisioning events.

Backout / Rollback Plan

1. TITAN auto-captured snapshot of app-telco-provisioning 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 app-telco-provisioning 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

```
az webapp log config --resource-group rg-telco-prov --name app-telco-provisioning  
--application-logging true --level information --retention-in-days 2555
```

Compliance Mapping

CIS Azure 6.2, NIST SC-7, PCI DSS 1.2.1, SOC 2 CC7.1

AI Close Notes

TITAN CONDUIT opened this high logging 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.

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