TITAN AI · CONDUIT · CHANGE REQUEST

CHG0030004 — [TITAN] Critical — security on afd-titan-frontend

Severity	Critical	Priority	1 - Critical
Cloud	Azure	State	New
Resource	afd-titan-frontend	Group	network_operations
Resource type	Microsoft.Network/frontDoors	Change type	Normal
Opened	2026-04-21 14:36:43	Closed	2026-04-21 14:36:43
CAB required	Yes	Close code	—

Security Finding

```
Azure Front Door publicly accessible with WAF policy disabled — open to L7 attacks and OWASP Top 10.
```

Justification

```
Azure Front Door publicly accessible with WAF policy disabled — open to L7 attacks and OWASP Top 10.
```

Implementation Plan

```
1. Pre-change snapshot captured by TITAN (auto-rollback available).
2. Execute fix command:
az network front-door waf-policy create --name wafp-titan --resource-group rg-titan-demo --mode Prevention
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 (afd-titan-frontend).
Blast radius: change is idempotent; pre-change snapshot captured by TITAN; auto-rollback available if rescan fails.
Finding detail: Azure Front Door publicly accessible with WAF policy disabled — open to L7 attacks and OWASP Top 10.
```

Backout / Rollback Plan

```
1. TITAN auto-captured snapshot of afd-titan-frontend 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 afd-titan-frontend 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 network front-door waf-policy create --name wafp-titan --resource-group rg-titan-demo --mode Prevention
```

Compliance Mapping

```
CIS 1.x IAM, NIST AC-2, SOC 2 CC6.1
```

AI Close Notes

```
(empty)
```