

INC0010112 — [TITAN] Critical — identity on aad-sp-telco-neta-analytics

Severity	Critical	Priority	1 - Critical
Cloud	Azure	State	Closed
Resource	aad-sp-telco-neta-analytics	Group	identity_and_access
Resource type	Microsoft.AAD/servicePrincipal	Change type	Emergency
Opened	2026-04-22 19:07:25	Closed	2026-04-22 19:21:25
CAB required	Yes	Close code	Successful

Security Finding

Network-analytics service principal has Directory.ReadWrite.All on Graph – can read every employee credential and MFA status. Privileged-access review overdue by 180 days.

Justification

Critical: Network-analytics service principal has Directory.ReadWrite.All on Graph – can read every employee credential and MFA status. Privileged-access review overdue by 180 days.

Implementation Plan

1. Pre-change snapshot captured by TITAN (auto-rollback available).
2. Execute fix command:
`az ad sp credential reset --id <sp-obj-id> --years 1 && az ad app permission remove --id <app-id> --api 00000003-0000-0000-c000-000000000000 --api-permissions 19dbc75e-c2e2-444c-a770-ec69d8559fc7=Role`
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 (aad-sp-telco-neta-analytics).
Blast radius: change is idempotent; pre-change snapshot captured by TITAN; auto-rollback available if rescan fails.
Finding detail: Network-analytics service principal has Directory.ReadWrite.All on Graph – can read every employee credential and MFA status. Privileged-access review overdue by 180 days.

Backout / Rollback Plan

1. TITAN auto-captured snapshot of aad-sp-telco-neta-analytics 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 aad-sp-telco-neta-analytics 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 ad sp credential reset --id <sp-obj-id> --years 1 && az ad app permission remove --id <app-id>
--api 00000003-0000-0000-c000-000000000000 --api-permissions
19dbc75e-c2e2-444c-a770-ec69d8559fc7=Role
```

Compliance Mapping

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

AI Close Notes

TITAN CONDUIT orchestrated end-to-end: SCOUT detected the critical identity incident, FORGE applied the consent-gated fix automatically (incident class), SCOUT rescan confirmed the finding cleared, and CONDUIT closed this ticket with a Successful close_code. Pre-change snapshot retained for 30 days for rollback.