

INC0010009 — [TITAN] Medium — security on mi-orphan-app1

Severity	Medium	Priority	4 - Low
Cloud	Azure	State	New
Resource	mi-orphan-app1	Group	identity_and_access
Resource type	Microsoft.ManagedIdentity/userAssignedIdentities	Category	Incident
Opened	2026-04-21 15:28:20	Closed	2026-04-21 15:28:20
CAB required	No	Close code	—

Security Finding

Managed identity 'mi-orphan-app1' has no role assignments for past 90 days. Orphaned credentials widen attack surface.

Justification

Medium: Managed identity 'mi-orphan-app1' has no role assignments for past 90 days. Orphaned credentials widen attack surface.

Implementation Plan

1. Pre-change snapshot captured by TITAN (auto-rollback available).
2. Execute fix command:
az identity delete --name mi-orphan-app1 --resource-group rg-titan-demo (after confirming no consumers).
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 risk – weaker control, should be hardened.
Business impact if unremediated: Control weakness that compounds with other gaps.
Scope: single resource (mi-orphan-app1).
Blast radius: change is idempotent; pre-change snapshot captured by TITAN; auto-rollback available if rescan fails.
Finding detail: Managed identity 'mi-orphan-app1' has no role assignments for past 90 days. Orphaned credentials widen attack surface.

Backout / Rollback Plan

1. TITAN auto-captured snapshot of mi-orphan-app1 before change (baseline: titan-killer-20260421T222819Z).
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 mi-orphan-app1 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 identity delete --name mi-orphan-app1 --resource-group rg-titan-demo (after confirming no consumers).
```

Compliance Mapping

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

AI Close Notes

2026-04-21 15:28:20 - System Administrator (Work notes)
[TITAN CONDUIT] Incident auto-filed from security scan.
Detecting agent: unknown (scan titan-killer-20260421T222819Z).
Severity: Medium (priority 3).
This is a hygiene/access-control issue that does not require a CAB-gated change window. Assign to the listed team and resolve per their standard runbook. TITAN will auto-detect clearance on the next scan.