

CHG0030104 — [TITAN] Medium — legacy_eol on acr-retired-image-base

Severity	Medium	Priority	3 - Moderate
Cloud	Azure	State	Assigned
Resource	acr-retired-image-base	Group	security_engineering
Resource type	Microsoft.ContainerRegistry/registries/images	Images type	Normal
Opened	2026-04-22 19:55:27	Closed	2026-04-22 19:55:27
CAB required	No	Close code	—

Security Finding

Container base image 'centos:7' detected in ACR – CentOS 7 EOL 2024-06-30 (297 days). Used as base for 14 downstream application images currently deployed. Fails CIS Controls v8 7.3, NIST 800-53 CM-6.

Justification

Medium: Container base image 'centos:7' detected in ACR – CentOS 7 EOL 2024-06-30 (297 days). Used as base for 14 downstream application images currently deployed. Fails CIS Controls v8 7.3, NIST 800-53 CM-6.

Implementation Plan

1. Pre-change snapshot captured by TITAN (auto-rollback available).
2. Execute fix command:
Rebuild images from rockylinux:9 or almalinux:9. Update all 14 downstream Dockerfile FROM statements. Rolling deploy via existing CI/CD.
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 (acr-retired-image-base).
 Blast radius: change is idempotent; pre-change snapshot captured by TITAN; auto-rollback available if rescan fails.
 Finding detail: Container base image 'centos:7' detected in ACR – CentOS 7 EOL 2024-06-30 (297 days). Used as base for 14 downstream application images currently deployed. Fails CIS Controls v8 7.3, NIST 800-53 CM-6.

Backout / Rollback Plan

1. TITAN auto-captured snapshot of acr-retired-image-base before change (baseline: titan-legacy-demo-20260422T201927Z).
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 acr-retired-image-base 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

Rebuild images from rockylinux:9 or almalinux:9. Update all 14 downstream Dockerfile FROM statements. Rolling deploy via existing CI/CD.

Compliance Mapping

CIS Benchmark, SOC 2 CC6.1

AI Close Notes

TITAN CONDUIT opened this medium legacy_eol change request and assigned it to the security_engineering 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