

CHG0030111 — [TITAN] Medium — legacy_eol on ec2-rhel6-billing-stack

Severity	Medium	Priority	3 - Moderate
Cloud	AWS	State	Assigned
Resource	ec2-rhel6-billing-stack	Group	security_engineering
Resource type	AWS::EC2::Instance	Change type	Normal
Opened	2026-04-22 19:13:27	Closed	2026-04-22 19:13:27
CAB required	No	Close code	—

Security Finding

RHEL 6 Server detected – past end-of-life 2020-11-30, past ELS (Extended Life-cycle Support) 2024-06-30. Runs telecom billing stack with CPNI data. Fails CPNI 47 CFR §64.2011, NIST 800-53 SI-2, ISO 27001 A.12.6.1, CIS Controls v8 7.3.

Justification

Medium: RHEL 6 Server detected – past end-of-life 2020-11-30, past ELS (Extended Life-cycle Support) 2024-06-30. Runs telecom billing stack with CPNI data. Fails CPNI 47 CFR §64.2011, NIST 800-53 SI-2, ISO 27001 A.12.6.1, CIS Controls v8 7.3.

Implementation Plan

1. Pre-change snapshot captured by TITAN (auto-rollback available).
2. Execute fix command:
In-place upgrade to RHEL 8/9 via Leapp utility, OR lift-and-shift to Amazon Linux 2023.
Compensating: no new package install, file-integrity monitoring, CloudWatch log forwarding.
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 (ec2-rhel6-billing-stack).
Blast radius: change is idempotent; pre-change snapshot captured by TITAN; auto-rollback available if rescan fails.
Finding detail: RHEL 6 Server detected – past end-of-life 2020-11-30, past ELS (Extended Life-cycle Support) 2024-06-30. Runs telecom billing stack with CPNI data. Fails CPNI 47 CFR §64.2011, NIST 800-53 SI-2, ISO 27

Backout / Rollback Plan

1. TITAN auto-captured snapshot of ec2-rhel6-billing-stack 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 ec2-rhel6-billing-stack 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

In-place upgrade to RHEL 8/9 via Leapp utility, OR lift-and-shift to Amazon Linux 2023.
Compensating: no new package install, file-integrity monitoring, CloudWatch log forwarding.

Compliance Mapping

CIS Azure 6.2, NIST SC-7, PCI DSS 1.2.1

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