

CHG0030107 — [TITAN] Critical — legacy_eol on esxi-host-prod-cluster-05

Severity	Critical	Priority	1 - Critical
Cloud	Multi	State	Assigned
Resource	esxi-host-prod-cluster-05	Group	security_engineering
Resource type	VMware::ESXi::Host	Change type	Emergency
Opened	2026-04-22 19:37:27	Closed	2026-04-22 19:37:27
CAB required	Yes	Close code	—

Security Finding

VMware ESXi 6.5 U3 detected on 8-node production cluster – past end-of-life 2022-10-15 (554 days). Hosts 142 production VMs including PCI-scope workloads. Fails PCI DSS 6.2, HIPAA 164.308(a)(5)(ii)(B), SOC 2 CC7.1.

Justification

Critical: VMware ESXi 6.5 U3 detected on 8-node production cluster – past end-of-life 2022-10-15 (554 days). Hosts 142 production VMs including PCI-scope workloads. Fails PCI DSS 6.2, HIPAA 164.308(a)(5)(ii)(B), SOC 2 CC7.1.

Implementation Plan

1. Pre-change snapshot captured by TITAN (auto-rollback available).
2. Execute fix command:
Upgrade to ESXi 8.0 U2 (supported until 2027) or migrate workloads to Azure/AWS/GCP. Interim: apply VMware's final security patches, isolate vCenter from untrusted networks.
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 (esxi-host-prod-cluster-05).
Blast radius: change is idempotent; pre-change snapshot captured by TITAN; auto-rollback available if rescan fails.
Finding detail: VMware ESXi 6.5 U3 detected on 8-node production cluster – past end-of-life 2022-10-15 (554 days). Hosts 142 production VMs including PCI-scope workloads. Fails PCI DSS 6.2, HIPAA 164.308(a)(5)(ii)(B)

Backout / Rollback Plan

1. TITAN auto-captured snapshot of esxi-host-prod-cluster-05 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 esxi-host-prod-cluster-05 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

Upgrade to ESXi 8.0 U2 (supported until 2027) or migrate workloads to Azure/AWS/GCP. Interim: apply VMware's final security patches, isolate vCenter from untrusted networks.

Compliance Mapping

CIS Benchmark, SOC 2 CC6.1

AI Close Notes

TITAN CONDUIT opened this critical 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