

CHG0030102 — [TITAN] High — legacy_eol on sqlsrv-core-ledger-prod

| | | | |
|---------------|-------------------------|-------------|----------------------|
| Severity | High | Priority | 2 - High |
| Cloud | Azure | State | Assigned |
| Resource | sqlsrv-core-ledger-prod | Group | security_engineering |
| Resource type | Microsoft.Sql/servers | Change type | Normal |
| Opened | 2026-04-22 20:07:27 | Closed | 2026-04-22 20:07:27 |
| CAB required | Yes | Close code | — |

Security Finding

SQL Server 2012 Enterprise detected – past end-of-life 2022-07-12 (651 days). ESU eligible but not enrolled. Hosts core banking ledger with CHD + SOX-relevant financial data. Fails PCI DSS 3.4 + 6.2, SOX ITGC-CM, FFIEC CAT, SOC 2 CC8.1.

Justification

High: SQL Server 2012 Enterprise detected – past end-of-life 2022-07-12 (651 days). ESU eligible but not enrolled. Hosts core banking ledger with CHD + SOX-relevant financial data. Fails PCI DSS 3.4 + 6.2, SOX ITGC-CM, FFIEC CAT, SOC 2 CC8.1.

Implementation Plan

1. Pre-change snapshot captured by TITAN (auto-rollback available).
2. Execute fix command:
Option 1: Enroll in SQL Server 2012 ESU (available until July 2025). Option 2: Migrate to Azure SQL Managed Instance. Compensating controls: TDE, network isolation, MFA, session monitoring.
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-HIGH risk – misconfiguration with realistic exploit path.
 Business impact if unremediated: Increases attack surface; auditor finding likely.
 Scope: single resource (sqlsrv-core-ledger-prod).
 Blast radius: change is idempotent; pre-change snapshot captured by TITAN; auto-rollback available if rescan fails.
 Finding detail: SQL Server 2012 Enterprise detected – past end-of-life 2022-07-12 (651 days). ESU eligible but not enrolled. Hosts core banking ledger with CHD + SOX-relevant financial data. Fails PCI DSS 3.4 + 6.2,

Backout / Rollback Plan

1. TITAN auto-captured snapshot of sqlsrv-core-ledger-prod 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 sqlsrv-core-ledger-prod 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

Option 1: Enroll in SQL Server 2012 ESU (available until July 2025). Option 2: Migrate to Azure SQL Managed Instance. Compensating controls: TDE, network isolation, MFA, session monitoring.

Compliance Mapping

CIS Benchmark, SOC 2 CC6.1

AI Close Notes

TITAN CONDUIT opened this high 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