CHG0030110 — [TITAN] High — legacy_eol on rds-sqlserver-2008r2-pastsu

Severity	High	Priority	2 - High
Cloud	AWS	State	Assigned
Resource	rds-sqlserver-2008r2-pastsu	Group	security_engineering
Resource type	AWS::RDS::DBInstance	Change type	Normal
Opened	2026-04-22 19:19:27	Closed	2026-04-22 19:19:27
CAB required	Yes	Close code	—

Security Finding

```
SQL Server 2008 R2 detected on RDS — past end-of-life AND past ESU (2022-07-12). Holds student records (FERPA). No further Microsoft or AWS patches will be issued. Fails FERPA §99.31, NIST 800-53 SI-2, ISO 27001 A.12.6.1, SOC 2 CC7.1.
```

Justification

```
High: SQL Server 2008 R2 detected on RDS — past end-of-life AND past ESU (2022-07-12). Holds student records (FERPA). No further Microsoft or AWS patches will be issued. Fails FERPA §99.31, NIST 800-53 SI-2, ISO 27001 A.12.6.1, SOC 2 CC7.1.
```

Implementation Plan

```
1. Pre-change snapshot captured by TITAN (auto-rollback available).
2. Execute fix command:
Upgrade to SQL Server 2022 on RDS or migrate to Aurora PostgreSQL. Compensating until cutover: VPC-only access, IAM DB auth, enhanced monitoring every 1s, database activity streams to S3.
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 (rds-sqlserver-2008r2-pastsu).
Blast radius: change is idempotent; pre-change snapshot captured by TITAN; auto-rollback available if rescan fails.
Finding detail: SQL Server 2008 R2 detected on RDS — past end-of-life AND past ESU (2022-07-12). Holds student records (FERPA). No further Microsoft or AWS patches will be issued. Fails FERPA §99.31, NIST 800-53 SI-2
```

Backout / Rollback Plan

```
1. TITAN auto-captured snapshot of rds-sqlserver-2008r2-pastsu 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 rds-sqlserver-2008r2-pastsu 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 SQL Server 2022 on RDS or migrate to Aurora PostgreSQL. Compensating until cutover:
VPC-only access, IAM DB auth, enhanced monitoring every 1s, database activity streams to S3.
```

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.
```