CHG0030101 — [TITAN] Critical — legacy_eol on ec2-exchange-2013-prod

Severity	Critical	Priority	1 - Critical
Cloud	AWS	State	Assigned
Resource	ec2-exchange-2013-prod	Group	security_engineering
Resource type	AWS::EC2::Instance	Change type	Emergency
Opened	2026-04-22 20:13:27	Closed	2026-04-22 20:13:27
CAB required	Yes	Close code	—

Security Finding

```
Microsoft Exchange Server 2013 CU23 detected via EWS + OWA banner — past end-of-life 2023-04-11
(380 days). No ESU path exists for Exchange 2013. Internet-exposed on port 443. Fails HIPAA
164.312(e)(1), PCI DSS 6.2, SOC 2 CC7.1, NYDFS 500 §500.07.
```

Justification

```
Critical: Microsoft Exchange Server 2013 CU23 detected via EWS + OWA banner — past end-of-life
2023-04-11 (380 days). No ESU path exists for Exchange 2013. Internet-exposed on port 443. Fails
HIPAA 164.312(e)(1), PCI DSS 6.2, SOC 2 CC7.1, NYDFS 500 §500.07.
```

Implementation Plan

```
1. Pre-change snapshot captured by TITAN (auto-rollback available).
2. Execute fix command:
Migrate mailboxes to Exchange Online (M365) or Exchange Server 2019. Interim: block OWA
externally, keep ActiveSync only, apply post-CU23 community patches.
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 (ec2-exchange-2013-prod).
Blast radius: change is idempotent; pre-change snapshot captured by TITAN; auto-rollback available
if rescan fails.
Finding detail: Microsoft Exchange Server 2013 CU23 detected via EWS + OWA banner — past
end-of-life 2023-04-11 (380 days). No ESU path exists for Exchange 2013. Internet-exposed on port
443. Fails HIPAA 164.312(e)(1
```

Backout / Rollback Plan

```
1. TITAN auto-captured snapshot of ec2-exchange-2013-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 ec2-exchange-2013-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

Migrate mailboxes to Exchange Online (M365) or Exchange Server 2019. Interim: block OWA externally, keep ActiveSync only, apply post-CU23 community patches.

Compliance Mapping

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

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.