CHG0030108 — [TITAN] Medium — legacy_eol on cisco-asa-fw-edge-01

Severity	Medium	Priority	3 - Moderate
Cloud	Multi	State	Assigned
Resource	cisco-asa-fw-edge-01	Group	security_engineering
Resource type	Cisco::ASA::5525X	Change type	Normal
Opened	2026-04-22 19:31:27	Closed	2026-04-22 19:31:27
CAB required	No	Close code	—

Security Finding

```
Cisco ASA 9.1(7)32 firmware detected on perimeter firewall — past end-of-life 2022-08-31 (601 days). No further security patches will be issued. Exposed CVE-2024-20481 unpatchable. Fails NIST 800-53 SC-7, CIS Controls v8 Control 12, PCI DSS 1.1.
```

Justification

```
Medium: Cisco ASA 9.1(7)32 firmware detected on perimeter firewall — past end-of-life 2022-08-31 (601 days). No further security patches will be issued. Exposed CVE-2024-20481 unpatchable. Fails NIST 800-53 SC-7, CIS Controls v8 Control 12, PCI DSS 1.1.
```

Implementation Plan

```
1. Pre-change snapshot captured by TITAN (auto-rollback available).
2. Execute fix command:
Replace with Cisco Firepower 2100 series or Palo Alto PA-400 (current firmware). Interim: subscribe to Cisco PSIRT advisories, compensating IDS behind the firewall.
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 (cisco-asa-fw-edge-01).
Blast radius: change is idempotent; pre-change snapshot captured by TITAN; auto-rollback available if rescan fails.
Finding detail: Cisco ASA 9.1(7)32 firmware detected on perimeter firewall — past end-of-life 2022-08-31 (601 days). No further security patches will be issued. Exposed CVE-2024-20481 unpatchable. Fails NIST 800-53 S
```

Backout / Rollback Plan

```
1. TITAN auto-captured snapshot of cisco-asa-fw-edge-01 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 cisco-asa-fw-edge-01 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

```
Replace with Cisco Firepower 2100 series or Palo Alto PA-400 (current firmware). Interim:
subscribe to Cisco PSIRT advisories, compensating IDS behind the firewall.
```

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.
```