INC0010106 — [TITAN] High — identity on iam-role-banking-crossaccount

Severity	High	Priority	2 - High
Cloud	AWS	State	Closed
Resource	iam-role-banking-crossaccount	Group	identity_and_access
Resource type	AWS::IAM::Role	Change type	Incident
Opened	2026-04-22 19:43:22	Closed	2026-04-22 19:57:22
CAB required	Yes	Close code	Successful

Security Finding

```
Cross-account IAM role trust policy uses wildcard principal (*). Any AWS account can assume this role — critical lateral-movement risk for banking workloads. SOX ITGC and FFIEC violation.
```

Justification

```
High: Cross-account IAM role trust policy uses wildcard principal (*). Any AWS account can assume this role — critical lateral-movement risk for banking workloads. SOX ITGC and FFIEC violation.
```

Implementation Plan

```
1. Pre-change snapshot captured by TITAN (auto-rollback available).
2. Execute fix command:
aws iam update-assume-role-policy --role-name banking-crossaccount --policy-document
file://fixed-trust-policy.json
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 (iam-role-banking-crossaccount).
Blast radius: change is idempotent; pre-change snapshot captured by TITAN; auto-rollback available
if rescan fails.
Finding detail: Cross-account IAM role trust policy uses wildcard principal (*). Any AWS account
can assume this role — critical lateral-movement risk for banking workloads. SOX ITGC and FFIEC
violation.
```

Backout / Rollback Plan

```
1. TITAN auto-captured snapshot of iam-role-banking-crossaccount before change (baseline:
titan-banking-demo-20260422T201922Z).
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 iam-role-banking-crossaccount 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

```
aws iam update-assume-role-policy --role-name banking-crossaccount --policy-document
file://fixed-trust-policy.json
```

Compliance Mapping

```
CIS 1.x IAM, NIST AC-2, SOC 2 CC6.1
```

AI Close Notes

```
TITAN CONDUIT orchestrated end-to-end: SCOUT detected the high identity incident, FORGE applied
the consent-gated fix automatically (incident class), SCOUT rescan confirmed the finding cleared,
and CONDUIT closed this ticket with a Successful close_code. Pre-change snapshot retained for 30
days for rollback.
```